EXHIBIT F

(Second Witness Statement of V. Pandey)

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-CV-954

FARHAD AZIMA, Plaintiff, v. NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC., Defendants.	)	**DECLARATION OF VIKASH K. PANDEY**

I, **VIKASH K. PANDEY**, do hereby declare under penalty of perjury pursuant to 28 U.S.C § 1746 the following:

1. I am an information technology and cybersecurity professional. I am also a former employee of CyberRoot Risk Advisory Private Limited ("**CyberRoot**"). CyberRoot is an Indian company that provides risk mitigation, online reputation management, information security, and digital forensics services. I worked at CyberRoot from approximately July 2016 until May 2020.

2. Unless otherwise stated, the facts set out below are within my own knowledge or are derived from other sources or documents that I have seen and which in all cases I believe to be true. Where any facts are not within my knowledge, the source of those facts is stated.

VKP.
Initials

My contacts with Mr. Farhad Azima and his Agents

3. In August 2020, I was contacted (via call) by one Mr. Jain ("**Mr. Jain**"), who told me he was approaching me on behalf of Mr. Azima and his solicitors, Burlington Legal LLP. Mr. Jain said he was engaged to act as an intermediary for Mr. Dominic Holden ("**Mr. Holden**"). Mr. Jain also falsely accused me of being involved in alleged hacking of Mr. Azima. I had not, prior to this, ever heard of Mr. Azima, nor did I know what Mr. Jain was talking about when he said Mr. Azima had been hacked.

4. Mr. Jain warned me that I was the primary suspect in an investigation into the hacking of Mr. Azima. Mr. Jain said he had discovered my involvement because another employee of CyberRoot and BellTroX Info Tech Services ("**BellTroX**") had used my name in the alleged hacking of Mr. Azima. Mr. Jain did not identify the employee who allegedly used my name. Again, at the time I did not know what Mr. Jain was talking about.

5. I immediately denied the accusations and dismissed them as either a mistake or a fabrication. For the avoidance of doubt:

a. Prior to these allegations, I did not know Mr. Azima;

b. I did not hack or assist in the alleged hacking of Azima;

c. I did not, either whilst employed by CyberRoot or otherwise, work on any projects directed at or related to Mr. Azima;

d. I do not know who hacked Mr. Azima or even if Mr. Azima was hacked, nor have I ever told some that I did have such knowledge;

VKP
Initials

e. During the time when I worked at CyberRoot, CyberRoot did not engage in any illegal hacking activities; and

f. I also believe, based on my time working there and knowing the directors well, that CyberRoot would not be, or have ever been, involved in illegal hacking operations, including the alleged hacking of Mr. Azima.

Demand Letters and Threats of Legal Action

6. On August 28, 2020, I received a demand letter from Mr. Holden on behalf of Azima. A true and accurate copy of Mr. Holden's demand letter, which is dated August 20, 2020, is attached hereto as **Exhibit A**.

7. In that letter, Mr. Holden claimed to be in possession of information that I was instrumental in the alleged hacking of Azima. While Mr. Holden did not, in that letter, disclose what information Mr. Azima possessed, he offered me "*a single opportunity to cooperate*" with his investigation and to provide a witness statement "*to avoid criminal and legal proceedings*."

8. As I explain in more detail below, I note that, as on the date I received Mr. Holden's letter, Mr. Jonas Rey has claimed in his witness statement that I had already divulged to him all there was to know about the hacking of Mr. Azima (which I did not do), including who was responsible and how it had been perpetrated.

9. Upon receiving Mr. Holden's demand letter, I immediately called a former colleague at CyberRoot – Mr. Chiranshu Ahuja ("**Mr. Ahuja**") – to determine whether he was aware of any security projects that related to Mr. Azima or work that could have been

VKP.
Initials

mistaken for the illegal acts of which Mr. Holden accused me. I explained to Mr. Ahuja that I had not hacked Mr. Azima and that I did not believe that CyberRoot engaged in any illegal activity. I also confirmed my recollection that CyberRoot did not work on matters related to Mr. Azima. Mr. Ahuja agreed with my recollection and told me that Mr. Holden must have been mistaken.

10. Given his prior warning to me, I also called Mr. Jain to notify him that I had received Holden's demand letter to ask why they were falsely accusing me of hacking Mr. Azima. Mr. Jain was aware of Holden's demand letter and told me that he would coordinate with Mr. Holden regarding the demand that I provide testimony (which I was told would remain anonymous) to avoid legal proceedings. While I did not fully understand Mr. Jain and Mr. Holden's request at the time, it is now my understanding that they intended for me to provide testimony favorable to their case to avoid civil and criminal proceedings.

11. On August 31, 2020, Mr. Holden sent me an email which attached a Confidentiality Agreement. A true and accurate copy of the Confidentiality Agreement is attached hereto as **Exhibit B**. I also received the same agreement from Mr. Jain (who said he was acting as Mr. Holden's "translator"). At that time, my father was unwell and was receiving treatment in hospital.

12. Over the next few days, Mr. Jain and Mr. Holden pressured me to sign the Confidentiality Agreement. I was told that Mr. Holden would only share the information supporting their accusations against me if I signed the Confidentiality Agreement. Mr. Jain also urged me sign the Confidentiality Agreement because – he said – Mr. Azima's

JKP.
Initials

representatives, including Mr. Holden, would immediately commence criminal and civil legal proceedings against me if I did not comply.

13. After several days of pressuring by Mr. Holden and Mr. Jain, I explained that I could not sign the Confidentiality Agreement because I was with my father who was sick and did not have access to a printer. I never did, in fact, sign the Confidentiality Agreement. However, I believe that Mr. Jain signed the Confidentiality Agreement with my name on September 2, 2020.

14. I feared that cooperating with Mr. Holden was the only way that I could confront the evidence that apparently supported his false accusations. Therefore, Mr. Jain signed the Confidentiality Agreement in my name. My agreement to sign the Confidentiality Agreement was obtained under duress and false pretenses, as Mr. Azima's representatives refused to provide any evidence to support their accusations.

15. On September 2, 2020, I attended a Zoom audio call (arranged by Mr. Jain) between me, Mr. Jain, and a legal representative of Mr. Azima. I do not know Mr. Holden's voice, so I cannot confirm whether he was on this call. However, I understood and reasonably believe that I spoke to Mr. Holden or another member of Mr. Azima's legal team with Burlington during that call.

16. During this call, the legal representative told me that I needed to admit to being instrumental to the hacking of Mr. Azima. He also claimed that he had evidence against me related to the hacking of Mr. Azima and accused me of being associated with

VKP.
Initials

BellTroX, a company which he claimed was also responsible for the hacking of Mr. Azima. None of those accusations were true and I said as much on the call.

17. For the avoidance of doubt:

a. I am not and have never been associated with BellTroX;

b. As set out above, I was not and have never been involved in the hacking of Mr. Azima; and

c. Prior to the accusations then being made, I did not know anything about the hacking of Mr. Azima.

18. I then demanded that I be provided with the evidence against me that was promised to me if I signed the Confidentiality Agreement. Reneging on that promise, Mr. Jain and the legal representative however refused to provide any evidence of my involvement.

19. I formed the view then, which I still hold now, that neither Mr. Azima nor his representatives ever had any evidence to support their accusations against me (nor could they ever have had any because there is none). Rather, I believe that they insisted on the Confidentiality Agreement because they intended to pressure me to give false testimony during this call.

20. Despite the falsity of the accusations and my clear denial of them, they continued on the Zoom call to threaten criminal and other legal proceedings against me unless I agreed to provide testimony for Mr. Azima's benefit. They also promised me

VKP.
Initials

anonymity, immunity from legal proceedings and compensation if I provided testimony that I had already confirmed was false and implicated others. I refused to do so.

21. On September 4, 2020, Mr. Holden sent me an email which attached a draft "Consultancy Agreement" between me and Burlingtons LLP. True and accurate copies of messages sent by Mr. Holden using his Burlingtons email address, dominic.holden@burlingtons.legal, are attached hereto as **Exhibit C**. In that email, Mr. Holden continued to pressure me to sign it to avoid legal proceedings. Mr. Jain also sent me a copy of the Consultancy Agreement.

22. The draft of the Consultancy Agreement sent to me included false representations that I knew about the hacking of Mr. Azima. As I had no knowledge of or involvement in the hacking of Mr. Azima and had previously advised that I had no knowledge of or involvement in the hacking of Mr. Azima, I refused to sign.

23. Later that day, Mr. Holden provided by email a revised version of the "Consultancy Agreement" to me, which he had signed on behalf of Burlingtons. Mr. Jain also sent me a copy of the revised Consultancy Agreement. This version did not refer to me having any knowledge of the hacking, but rather that I had agreed to assist Burlingtons in relation to their investigation.

24. Both versions of the Consultancy Agreement indicated that I was risking my reputation and my "personal security" by assisting Burlingtons. True and accurate copies of the initial draft and revised draft of the Consultancy Agreement are attached hereto as **Exhibit D**.

SKP.
Initials

25. Mr. Holden and Mr. Jain repeatedly insisted that I implicate others, including CyberRoot, in the hacking of Mr. Azima in exchange for payment under the Consultancy Agreement. Mr. Holden demanded that I agree to statements that I had previously denied (and still deny) and for which Mr. Holden did not provide supporting evidence.

26. When I refused to sign the revised Consultancy Agreement, Mr. Holden, through Mr. Jain, continued to threaten legal action against me if I did not change my mind, and told me that I should focus on the money that I would be able to make if I signed the Consultancy Agreement. Mr. Jain told me that he had estimated that I would be paid INR 3.3 crore (over $500,000) if I signed the revised Consultancy Agreement.

27. Despite the pressure placed on me, I refused to sign the Consultancy Agreement; the information and admissions that Mr. Holden and Mr. Jain sought from me were false, and I understood that the proposed payments I was being offered to falsely implicate CyberRoot were intended to frame CyberRoot in the hacking of Mr. Azima, which I was not prepared to do.

28. After the repeated attempts to pressure me into implicating CyberRoot, I stopped communicating with Mr. Holden in early September 2020.

The Allegations Concerning Me in Mr. Azima's High Court Application

29. I have been provided with and read the 12th Witness Statement of Mr. Holden, dated February 12, 2021 ("Holden12"), as well as a copy of the witness statement of Jonas Rey, dated February 11, 2021. True and accurate copies of these witness statements are attached hereto as **Exhibit E**.

VKP.
Initials

30. Holden12 adopts and relies upon facts and matters set out by Mr. Rey in his statement but, in summary, it is said by both Mr. Holden and Mr. Rey that at some time between July 6, 2020 and mid-September 2020, Source 1 informed Rey that: (a) CyberRoot is a "hack for hire" firm, and (b) me and four others had directly worked on the hack of Azima whilst at CyberRoot.

31. I address below these allegations in more detail, but confirm that this is untrue. I cannot emphasize strongly enough how gravely false these accusations are. Mr. Rey's witness statement is, to the extent it concerns me and CyberRoot (as such matters only are within my knowledge), a fabrication.

The Witness Statement of Jonas Rey

32. At paragraph 12 of Mr. Rey's statement, he says that he was introduced to me by Rajat Shirish. This is not true. I have never met or spoken to Mr. Rey. Prior to being passed a copy of his witness statement, I had never heard of him. It follows that everything in Mr. Rey's statement which claims to have been learnt from me is false. None the less, I deal with each allegation for the avoidance of any doubt.

33. At paragraph 12 of Mr. Rey's statement, he says that I was a freelance sub contractor to CyberRoot from 2013. This is false. I never freelanced for CyberRoot.

34. At paragraph 14 of his statement, Mr. Rey says that he then "*proceeded to have direct communications*" with me including "*oral discussions*" and Zoom calls involving me, Mr. Shirish and someone he describes as "Source 1." Again, this is false. I have never had any "oral discussions" with Mr. Rey – either with Mr. Shirish or otherwise.

VKP
Initials

As set out above, I do not know, have never met and never spoken to Mr. Rey. For the avoidance of doubt, whilst I did work with Mr. Shirish at CyberRoot from April 1, 2019 to July 1, 2019 during that period I have never worked with him on hacking Mr. Azima or anyone else.

35. Mr. Rey also claims at paragraph 14 of his witness statement that he obtained information from me through "*written messages passing through Mr Shirish and Source 1.*" Again, and for the avoidance of any doubt, this is untrue. I have not sent (or received) any written messages in any form to Mr. Rey. As set out above, I do not know, have never met and never spoken to Mr. Rey. I note that Mr. Rey did not exhibit to his witness statement any of these alleged written messages. Mr. Rey seems to suggest (at footnote 5) that this is because he used "disappearing" messages through an unidentified communication application.

36. This explanation as to why Mr. Rey has no written communications to or from me is false. He has none because there were not any.

37. At paragraph 16 of his witness statement, Mr. Rey says that from his communications with me:

a. He "understands that a team of CyberRoot employees", in addition to me, were "engaged in attempting to hack Mr Azima's data and that different members of the team worked on this project at different times;

b. He understands that I began working on this project in approximately June or July 2015;

Initials

c. That others were working on the project earlier; and

d. That the CyberRoot team were initially unsuccessful.

38. As I explained above, I did not have any communications with Mr. Rey (either directly or indirectly) and so it follows that I did not tell him any of the above, which in any event is all false. I have never worked on a project to hack Mr. Azima and nor has CyberRoot.

39. At paragraphs 17, 18 and 19 of his witness statement, Mr. Rey makes various assertions about the hacking of Mr. Azima and others. I note that he does not, in those paragraphs, expressly say those assertions and knowledge are based on what I told him. This includes the allegation at paragraph 17 that CyberRoot were tasked by Mr. Nicholas Del Rosso ("Del Rosso") to hack someone else and (at paragraph 19) that Del Rosso requested CyberRoot to set up methods to monitor Mr. Azima's emails.

40. For the avoidance of doubt, and it follows from what I have said above, I did not give any such information to Mr. Rey. During my time working there (and I believe at all times), CyberRoot were never tasked by Del Rosso (or anyone else) to hack anyone or monitor Azima's emails. I do not know Del Rosso or Vital Management Services, Inc. ("**VMS**") and did not hear about them till the present case.

41. At paragraph 20, it is alleged that I was "*the developer responsible for developing the phishing infrastructure of CyberRoot*" and that I was "*directly responsible for designing the backbone infrastructure that was then used to conduct phishing and social engineering attacks on Mr Azima.*" Again, this is false. First, CyberRoot does not

Vap.
Initials

have *a "phishing infrastructure*." Second, and accordingly, I did not develop one. Third, CyberRoot did not use any such infrastructure to phish or otherwise attack Mr. Azima. I confirm, again, that I did not discuss or "*expand*" on these matters with Mr. Rey (or anyone else). I do not know Mr. Rey and I have never discussed anything with Mr. Rey.

42. At paragraphs 21 and 23, Rey alleges that I explained further matters to him in relation to the hacking of Mr. Azima. Again, I explained no such things to Mr. Rey (or anyone else). I have never spoken to Mr. Rey (or anyone else) about such matters.

43. At paragraph 24 of his statement, Mr. Rey says I explained that in 2015 and 2016 CyberRoot was "*initially lacking hacking infrastructure*" and as such, it had asked the founder of BellTrox, Mr. Gupta, to use their infrastructure. Mr. Rey then makes further assertions as to things I allegedly explained to him about how BellTrox was involved in the hacking. Mr. Rey makes similar allegations in paragraph 44.8 of his statement. Again, this is all false. I have never discussed such things with Mr. Rey (or anyone else). Further, I have never worked with BellTrox and do not know Gupta. During my time at CyberRoot, we never engaged in any hacking and never worked with BellTrox – either in the way described by Mr. Rey or otherwise.

44. At paragraphs 25 to 36 of his witness statement, Mr. Rey makes several further assertions about things I have supposedly told him about CyberRoot's and VMS's role in the hacking of Mr. Azima. As I have explained above, all that evidence is not true. Everything Mr. Rey says I have "*explained*" or "*confirmed*" to him is untrue. I have never

VEP.
Initials

said any such things – either orally or in writing – to Mr. Rey (or anyone else). I do not know anything about the alleged hacking of Mr. Azima.

45. At paragraph 37 of his statement, Mr. Rey says that I was initially very forthcoming with him, but then became increasingly concerned and became un-cooperative and refused to engage further. It is also said that I told him that I had been accused of manslaughter. This is a work of fiction, which I believe was introduced to discredit my response to Mr. Rey's false statements and my denial of any involvement in the hacking of Mr. Azima. To repeat myself, I have never met, spoken with or communicated with Mr. Rey. I have not been accused of manslaughter and I have no idea where that allegation comes from.

46. At paragraph 38 of his statement, Mr. Rey says that in the middle of September 2020, he was told by "Source 1" that I had disclosed my conversations with Mr. Rey to the management of CyberRoot. As I explained above, it was in September 2020 that Mr. Jain and Mr. Holden approached me to provide false evidence and it was at or around that time that I told CyberRoot's management what was going on. "Source 1" could not have told Mr. Rey that I had disclosed my conversations with Mr. Rey to CyberRoot because I never had any such conversations with anyone.

47. Mr. Rey refers in paragraph 39 of his witness statement to Mr. Azima filing a complaint in the US Courts against Mr. Del Rosso and VMS on October 15, 2020. That complaint (I later learned) alleged that Mr. Del Rosso and VMS had instructed CyberRoot to carry out the hacking of Mr. Azima. I had, prior to that, already told CyberRoot about

VRP
Initials

my interactions with Mr. Jain and Mr. Holden (referred to above) and that they had accused me and CyberRoot of being involved in the hacking of Mr. Azima.

48. When the US complaint was issued, the legal representatives for Mr. Del Rosso and VMS asked me if I would be prepared to make a "declaration" for potential future use in those US legal proceedings. I agreed that I would and I signed the declaration on October 22, 2020. A true and accurate copy of the declaration that I executed on October 22, 2020 – including exhibits that I authenticated at that time – is attached hereto as **Exhibit F**. I did so entirely voluntarily, without any remuneration or other financial benefit, or expectation that I would receive any remuneration or financial benefit. Notably, my prior declaration set out clear denials regarding my alleged involvement in the hacking of Mr. Azima. I obviously had not seen, in October 2020, the expanded allegations which have since been made against me personally in Mr. Rey's statement in February 2021.

49. At paragraph 40, Mr. Rey says that "Source 1" told him that I had approached CyberRoot and asked them to support me if I "got into legal trouble" following the work I did for CyberRoot. I cannot say whether this is what "Source 1" told Mr. Rey. I can however confirm that I have had no such conversations with CyberRoot, not least because I did not do anything whilst working at CyberRoot that would cause me any legal trouble.

50. At paragraph 41 of his statement, Mr. Rey says that "Source 1" has told him that CyberRoot have "*reportedly*" offered me a "*substantial sum*" and "*a percentage in the equity*" of CyberRoot, if I decided to "*side with them.*" Again, I cannot comment as to

VLP.
Initials

whether this is what "Source 1" told Rey, or who has apparently "reported" this to "Source 1". I can, however, confirm that CyberRoot has not offered me any money or other financial benefit to "*side with them*", nor do I think I am siding with anyone. As noted above, Mr. Azima and his representatives are the only persons who have offered me financial compensation to participate in this matter. I voluntarily provided my prior declaration because what has been alleged by Mr. Azima and his representatives is false.

51. At paragraph 42 of his statement, Mr. Rey says he understands from "Source 1" that CyberRoot's directors have told all former employees not to speak to anyone about previous work they have done and tried to scare them. I cannot speak for all former employees, but I can confirm that CyberRoot has not told me not to talk to anyone in this regard, nor have they tried to scare me into not doing so.

The Twelfth Witness Statement of Dominic Holden

52. At paragraph 39 of Holden12, he says that the evidence of Mr. Rey is "*based on statements and admissions by the individuals at CyberRoot involved in hacking.*" For the reasons set out above, Mr. Holden's conclusion is fundamentally false and to the extent he is referring to admissions apparently made by me, his is wrong. I appreciate that Holden is apparently relying on Mr. Rey's evidence in making such a statement. However, I have explained above that Mr. Holden was – directly and indirectly, in discussions with me up to early September 2020 about these matters.

53. According to Mr. Rey, by that time – and in the period since July 6, 2020 – I had already "*boasted*" about my involvement in the hacking of Mr. Azima and disclosed

VBP
Initials

to him and Mr. Jain all the details as to how the hacking had come about. But at the same time as I was apparently freely giving all that information, Mr. Holden knew I had refused to sign the Consultancy Agreement and had not even been told by Mr. Holden or Mr. Jain what I had allegedly done. I do not understand, therefore, why Mr. Holden has endorsed Mr. Rey's evidence or at the very least not questioned it.

Executed on March 25, 2021 in Delhi, India.

Vikash.

Vikash K. Pandey

VKP.

Initials

Exhibit A

BURLINGTONS

MORE THAN LAW

Mr. Vikash Kumar Pandey
S/O Narmda Pasad Pandey, 272
N Pa Pasan, Pasan, Maharani
Laxmi Ward No 12, Kotma
Anuppur
Madhya Pradesh – 484336

Date: 20 August 2020
Our Ref: DH/AZI0003.2

Dear Sir,

RE: OUR CLIENT: MR. FARHAD AZIMA

We act for Mr. Farhad Azima.

Background

In August 2016, Mr. Azima's private and confidential data was published on the internet after it was illegally obtained by a cyber security hack (**"the Hack"**).

As a result of the dissemination of his data, he has suffered substantial damage to his reputation and earning potential. We estimate that his losses amount to in excess of $20,000,000.

Your role

We are in possession of information which confirms that you were involved and, indeed, were instrumental to the Hack. This is a very serious matter and you are liable to compensate Mr. Azima for the damage he has suffered as a result of the Hack.

We are however aware that you are not the sole player in the Hack and that you were performing your role on the instructions you had received from your client.

In the circumstances, we are offering you a single opportunity to co-operate with Mr. Azima's legal team to reveal the identity of the client who instructed you to hack Mr. Azima and to provide a Witness Statement sworn by a statement of truth explaining (1) your role in the Hack (2) the means by which the Hack occurred and (3) on whose instructions you were acting.

You have 3 days on receipt of this letter to respond to this request. If we have not received a satisfactory reply that you will co-operate willingly, our client will proceed with legal proceedings against you.

[redacted] 5 Stratford Place, London W1C 1AX

Representative offices:
Almaty, Geneva, Gibraltar, Malta, Moscow, St. Petersburg

Tel: +44 (0) 207 529 5420
Fax: +44 (0) 207 495 7450
DX: 82986 Mayfair
Web: www.burlingtons.legal

We urge you to take legal advice on the contents and effect of this letter.

All our client's rights and remedies are reserved.

Yours faithfully,

Dominic Holden

BURLINGTONS LEGAL LLP

Exhibit B

STRICTLY PRIVATE, CONFIDENTIAL AND PRIVILEGED

Confidentiality Agreement

BURLINGTONS

5 Stratford Place, London, W1C 1AX
Tel: 0207 529 5420 Fax: 0207 495 7450
www.burlingtonsllp.com

Ref: DH/AZI

CONTENTS

CLAUSE

This agreement is dated .....

Parties

(1) Burlingtons Legal LLP incorporated and registered in England and Wales with company number OC360876 whose registered office is at 5 Stratford Place, London, W1C 1AX (**Party 1**).

(2) Vikash Kumar Pandey of S/O Narmda Prasad Pandey, 272 N Pa Pasan, Pasan, Maharani Laxmi Ward No 12, Kotma, Anuppur, Madhya Pradesh – 484336 (**Party 2**).

BACKGROUND

(A) The parties intend to enter into discussions relating to the Purpose which will involve the exchange of Confidential Information between them.

(B) The parties have agreed to comply with this agreement in connection with the disclosure and use of Confidential Information.

Agreed terms

1. Interpretation

1.1 Definitions:

Business Day: a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

Confidential Information: has the meaning given in clause 2.

Discloser: a party to this agreement when it discloses its Confidential Information, directly or indirectly, to the other party.

Group: in relation to a company, that company, any subsidiary or any holding company from time to time of that company, and any subsidiary from time to time of a holding company of that company. Each company in a Group is a member of the Group.

Group Company: in relation to a company, any member of its Group.

Holding company: has the meaning give in clause 1.2(e).

Purpose: to assist in relation to ongoing litigation (including arbitration and other forms of dispute resolution fora) concerning Party 1 and / or Party 1's clients.

Recipient: a party to this agreement when it receives Confidential Information, directly or indirectly, from the other party.

Representative(s): in relation to each party and any member of its Group:

a) its officers and employees that need to know the Confidential Information for the Purpose;

b) its professional advisers or consultants who are engaged to advise that party and/or any member of its Group in connection with the Purpose;

c) its contractors and sub-contractors engaged by that party and/or any member of its Group in connection with the Purpose; and

d) any other person to whom the other party agrees in writing that Confidential Information may be disclosed in connection with the Purpose.

Subsidiary: has the meaning given in clause 1.2(e).

1.2 Interpretation.

(a) A reference to a statute or statutory provision is a reference to it as amended or re-enacted. A reference to a statute or statutory provision includes any subordinate legislation made under that statute or statutory provision, as amended or re-enacted.

(b) Any words following the terms **including**, **include**, **in particular**, **for example** or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

(c) A reference to **writing** or **written** includes fax and email.

(d) A reference to a **company** shall include any company, corporation or other body corporate, wherever and however incorporated or established.

(e) A reference to a **holding company** or a **subsidiary** means a holding company or a subsidiary (as the case may be) as defined in section 1159 of the Companies Act 2006 and a company shall be treated, for the purposes only of the membership requirement contained in section 1159(1)(b) and (c), as a member of another company even if its shares in that other company are registered in the name of:

(i) another person (or its nominee) by way of security or in connection with the taking of security; or

(ii) its nominee.

(f) Any obligation on a party not to do something includes an obligation not to allow that thing to be done.

2. Confidential Information

2.1 Confidential Information means all confidential information relating to the Purpose which the Discloser or its Representatives or any of its Group Companies, or their

Representatives directly or indirectly discloses, or makes available, to the Recipient or its Representatives or any of its Group Companies, or their Representatives, before, on or after the date of this agreement. This includes:

(a) the fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations;

(b) the existence and terms of this agreement;

(c) all confidential or proprietary information relating to:

(i) the business, affairs, customers, clients, suppliers, plans, intentions, or market opportunities of the Discloser or of any of the Discloser's Group Companies; and

(ii) the operations, processes, product information, know-how, technical information, designs, trade secrets or software of the Discloser, or of any of the Discloser's Group Companies;

(d) any information, findings, data or analysis derived from Confidential Information; and

(e) any other information that is identified as being of a confidential or proprietary nature;

but excludes any information referred to in clause 2.2.

2.2 Information is not Confidential Information if:

(a) it is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by the Recipient or its Representatives or by any of the Recipient's Group Companies or their Representatives in breach of this agreement (except that any compilation of otherwise public information in a form not publicly known shall still be treated as Confidential Information);

(b) it was available to the Recipient on a non-confidential basis prior to disclosure by the Discloser;

(c) it was, is, or becomes available to the Recipient on a non-confidential basis from a person who, to the Recipient's actual knowledge, is not under any confidentiality obligation in respect of that information;

(d) it was lawfully in the possession of the Recipient before the information was disclosed by the Discloser; and

(e) the parties agree in writing that the information is not confidential.

3. Confidentiality obligations

3.1 In return for the Discloser making Confidential Information available to the Recipient, the Recipient undertakes to the Discloser that it shall:

(a) keep the Confidential Information secret and confidential;

(b) not use or exploit the Confidential Information in any way except for the Purpose;

(c) not disclose or make available any Confidential Information in whole or in part to any person, except as expressly permitted by, and in accordance with this agreement.

3.2 The Recipient shall establish and maintain adequate security measures (including any reasonable security measures proposed by the Discloser from time to time) to safeguard the Confidential Information from unauthorised access or use.

4. Permitted disclosure

4.1 Disclosure to Representatives.

(a) The Recipient may disclose the Confidential Information to its Representatives, any of its Group Companies, or their Representatives on the basis that it:

(i) informs those Representatives, Group Companies or their Representatives of the confidential nature of the Confidential Information before it is disclosed; and

(ii) takes reasonable steps to procure that those Representatives, Group Companies or their Representatives comply with the confidentiality obligations in clause 3.1 as if they were the Recipient.

(b) The Recipient shall be liable for the actions or omissions of the Representatives, any of its Group Companies or their Representatives in relation to the Confidential Information as if they were the actions or omissions of the Recipient.

5. Mandatory disclosure

5.1 Subject to the provisions of this clause 5, a party may disclose Confidential Information to the minimum extent required by:

(a) an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction;

(b) the rules of any listing authority or stock exchange on which its shares or those of any of its Group Companies are listed or traded; or

(c) the laws or regulations of any country to which its affairs or those of any of its Group Companies are subject.

6. Return or destruction of Confidential Information

6.1 At the reasonable written request of the Discloser, the Recipient shall:

(a) destroy all documents and materials containing, reflecting, incorporating or based on the Confidential Information; and

(b) to the extent legally and technically practicable, erase all the Confidential Information from its computer and communications systems and devices used by it, or which is stored in electronic form.

6.2 Nothing in clause **Error! Reference source not found.** shall require the Recipient to return or destroy any documents and materials containing or based on the Discloser's Confidential Information that the Recipient is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or the rules of any listing authority or stock exchange, to which it is subject. The provisions of this agreement shall continue to apply to any documents and materials retained by the Recipient pursuant to this clause 6.2.

7. No obligation to continue discussions

Nothing in this agreement shall impose an obligation on either party to continue discussions or negotiations in connection with the Purpose, or an obligation on each party, or any of its Group Companies to disclose any information (whether Confidential Information or otherwise) to the other party.

8. Ending discussions and duration of confidentiality obligations

8.1 If either party decides not to continue to be involved in the Purpose with the other party, it shall notify that other party in writing immediately.

8.2 Notwithstanding the end of discussions between the parties in relation to the Purpose pursuant to clause 8.1, each party's obligations under this agreement shall continue in full force and effect.

8.3 The end of discussions relating to the Purpose shall not affect any accrued rights or remedies to which either party is entitled.

9. No partnership or agency

9.1 Nothing in this agreement is intended to, or shall be deemed to, establish any partnership or joint venture between the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

9.2 Each party confirms it is acting on its own behalf and not for the benefit of any other person.

10. General

10.1 Assignment and other dealings. Neither party shall assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any of its rights and obligations under this agreement.

10.2 Entire agreement

(a) This agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

(b) Each party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this agreement. Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this agreement.

10.3 Variation. No variation of this agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

10.4 Waiver. No failure or delay by a party to exercise any right or remedy provided under this agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

10.5 Severance

(a) If any provision or part-provision of this agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this agreement.

10.6 Notices

(a) Any notice or other communication given to a party under or in connection with this agreement shall be in writing and shall be:

(i) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

(ii) sent by email to the following addresses:

(A) Party 1: *dominic.holden@burlingtons.legal*

(B) Party 2: *vikz.hax@gmail.com*

(b) Any notice or communication shall be deemed to have been received:

(i) if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address; and

(ii) if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting or at the time recorded by the delivery service; and

(iii) if sent by email, at the time of transmission, or, if this time falls outside business hours in the place of receipt, when business hours resume. In this Clause 10.6(b)(iii), business hours means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the place of receipt.

(c) This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

(d) A notice given under this agreement is not valid if sent by email.

10.7 **Third party rights**

(a) Unless it expressly states otherwise, this agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this agreement.

(b) The rights of the parties to rescind or vary this agreement are not subject to the consent of any other person.

10.8 Governing law. This agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

10.9 Jurisdiction. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

This agreement has been entered into on the date stated at the beginning of it.

Signed by Dominic Holden and on behalf of **Burlingtons Legal LLP**	..... Partner
Signed by **Vikash Kumar Pandey**	.....

Exhibit C

Dominic Holden 4 Sep

to me

From Dominic Holden • dominic.holden@burlingtons.legal

To vikz.hax@gmail.com

Date 4 Sep 2020, 11:34 pm

Standard encryption (TLS).
See security details

Show pictures

Dear Vikash,

Further to my email below, I attach signed Confidentiality Agreement / NDA.

Please sign and return the complete, signed version to me (scan and email is fine).

Show quoted text

Private, Confidential and Privileged - Subject to Contract

Inbox

Dominic Holden 4 Sep
to me

From Dominic Holden • dominic.holden@burlingtons.legal

To vikz.hax@gmail.com

Date 4 Sep 2020, 11:05 pm

Standard encryption (TLS).
See security details

Show pictures

Dear Vikash,

I attach our signed counterpart of the Consultancy Agreement.

Please could you sign and then return to me a copy of the complete signed version (scan and email is fine).

Please do not hesitate to telephone me to discuss – my contact details are below.

Kind regards,

Message

From: Dominic Holden [dominic.holden@burlingtons.legal]
Sent: 9/4/2020 1:35:34 PM
To: vikz.hax@gmail.com
Subject: Private, Confidential and Privileged - Subject to Contract
Attachments: 2020 09 04 Consultancy Agreement (signed by Burlingtons).pdf

Dear Vikash,

I attach our signed counterpart of the Consultancy Agreement.

Please could you sign and then return to me a copy of the complete signed version (scan and email is fine).

Please do not hesitate to telephone me to discuss – my contact details are below.

Kind regards,

Dominic Holden
Partner
Burlingtons

Tel: +44 (0) 207 529 5420
Mob: 07863174364
Email: dominic.holden@burlingtons.legal
Fax: +44 (0) 207 495 7450
DX: 82986 Mayfair

BURLINGTONS

5 Stratford Place, London, W1C 1AX

Exhibit D

VIKASH KUMAR PANDEY

- and -

BURLINGTONS LEGAL LLP

CONSULTANCY AGREEMENT

AGREEMENT IS MADE ON …… SEPTEMBER 2020

BETWEEN:

(1) **Vikash Kumar Pandey** of S/O Narmada Pasad Pandey, 272 N Pa Pasan, Pasan, Maharani Laxmi Ward No 12, Kotma Anuppur, Madhya Pradesh - 484336 (**"the Consultant"**); (**"the Consultant"**); and

(2) **Burlingtons Legal LLP** incorporated and registered in England & Wales with company number OC360876 whose registered office is at 5 Stratford Place, London W1C 1AX ("**Burlingtons**").

WHEREAS:

(A) The Consultant is an IT expert and ex-employee of of Cyber Root Risk Advisory Private Limited (**"CR"**).

(B) Burlingtons are the English solicitors acting for Mr. Azima who is the Defendant, Counterclaimant and Proposed Appellant in proceedings commenced by Ras Al Khaimah Investment Authority ("**RAKIA**") in the High Court in London under Claim No. HC-2016-002798 (the "**RAKIA Proceedings**"). The RAKIA Proceedings concern, amongst other matters, the hacking of Mr. Azima's emails in around 2015 / 2016 (**"the Hack"**).

(C) The Consultant has agreed to provide assistance to Burlingtons in relation to their investigation into the Hack (**"the Hacking Investigation"**).

(D) It is understood that by assisting Burlingtons with the Hacking Investigation (**"the Purpose"**) the Consultant is risking his reputation within the IT industry and his personal security and that the Consultant may be required to incur substantial costs to ensure that his personal security is protected.

(E) The Consultant has dedicated time, and will need to dedicate further time, to providing information and assistance in connection with the Hacking Investigation. It is agreed that the Consultant will be engaged for the Purpose on the terms set out below.

IT IS AGREED:

1. **INTERPRETATION**

1.1 In this Agreement:

"**Commencement Date**" means 1 August 2020;

"**Confidential Information**" means confidential or secret information relating to Mr. Azima and / or the Hacking Investigation, including, without limitation, the existence and terms of this Agreement and any communications between Burlingtons (and / or its agents and / or advisers) and the Consultant;

"**Services**" means the services described in clause 3.

1.2 In this Agreement, any reference to a statutory provision is a reference to the provision from time to time renumbered, amended, re-enacted or consolidated.

1.3 In this Agreement, unless the context otherwise requires:

(a) references to clauses are to clauses of this Agreement; and

(b) the headings to the clauses are for convenience only and do not affect the Agreement's construction or interpretation.

2. **APPOINTMENT**

2.1 With effect from the Commencement Date, Burlingtons has engaged the Consultant to perform the Services.

3. **SERVICES**

3.1 During his engagement under this Agreement, the Consultant will give information and assistance to Burlingtons and / or its agents in connection with the Hacking Investigation.

3.2 The Consultant acknowledges that this could involve, but is not limited to, assisting in relation to any regulatory or legal process, preparing witness statements and giving evidence in person.

3.3 Without prejudice to the generality of clause 3.1, the Consultant shall make himself available for meetings for up to 30 hours per calendar month (via Zoom or other form of agreed upon video conferring platform), such meetings to take place at Burlington's request upon giving the Consultant at least 3 business days' notice; and

3.4 The Consultant represents, warrants and agrees that:

(a) any information or assistance provided to Burlingtons pursuant to this Agreement will be complete and accurate, and will be given truthfully to the best of the Consultant's knowledge and belief.

(b) he is a former employee of CR and has direct knowledge of the Hack.

(c) The execution, delivery and performance of this agreement will not conflict with:-

(i) Any law or regulation applicable to him; and / or

(ii) Any agreement or instrument binding upon him.

3.5 The Consultant shall indemnify Burlingtons against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred arising out of or in connection with:-

(a) Any breach of the warranties contained in clause 3.4.

(b) Any breach of this agreement.

(c) The enforcement of this agreement.

(d) Any claim made against Burlingtons by a third party arising out of or in connection with the provision of the Services.

3.6 It is agreed that no information or documentation (except as required by an order of a court of competent jurisdiction, or pursuant to any proper order or demand made by any competent authority or body where Burlingtons is under a legal or regulatory obligation to disclose the information and / or documentation) provided by the Consultant pursuant to this Agreement will be used by Burlingtons (on behalf of Mr. Azima) in support of any, action, claim, or prosecution against the Consultant in relation to his liability for the Hack.

4. **REMUNERATION**

4.1 Subject to the terms of this Agreement, Burlingtons shall pay the Consultant the sum of $550 per hour (exclusive of any applicable VAT) in consideration for the provision of the Services for a period of at least 18 months.

4.2 Subject to Burlingtons' prior written approval, Burlingtons shall reimburse all reasonable expenses properly and necessarily incurred by the Consultant in the course of this Agreement, subject to production of receipts or other appropriate evidence of payment.

4.3 The payment referred to at paragraph 4.1 shall include all work undertaken and assistance provided to Burlingtons by the Consultant to the date of this Agreement.

4.4 The period of service referred to at paragraph 4.1 may be extended by written agreement between the parties.

5. **CONFIDENTIAL INFORMATION**

5.1 The Consultant will not, except with the prior written consent of Burlingtons or pursuant to an order of a court of competent jurisdiction, or pursuant to any proper order or demand made by any competent authority or body where the Consultant is under a legal or regulatory obligation to make such disclosure, or to the Consultant's lawyers, auditors or insurers on terms which preserve confidentiality:

(a) disclose or communicate to any person, firm or company;

(b) cause unauthorised disclosure of; or

(c) otherwise make use of,

any Confidential Information that he has or may have acquired in the course of his engagement (whether before, on or after the date of this Agreement) and will use his best endeavours to prevent the unauthorised disclosure or publication of such information. This obligation survives the termination of this Agreement.

5.2 The obligations in clause 5.1 will cease if the relevant Confidential Information comes into the public domain other than through the Consultant's default or negligence.

6. **TERMINATION**

6.1 Upon the termination of this Agreement for whatever reason, the Consultant will deliver up all property and any documents or other information belonging to Burlingtons (and / or to Mr. Azima), including any Confidential Information, whether held electronically or in hard copy, which is in the Consultant's possession or under his control. The Consultant will not retain any copies of any such property, documents or information without written permission from Burlingtons.

6.2 The termination of this Agreement will not affect any of the provisions of this Agreement that are expressed to operate or have effect after its termination (including without limitation clause 5.1) and will not prejudice the exercise of any right or remedy of either party that has accrued prior to termination.

7. **STATUS**

7.1 The relationship of the Consultant to Burlingtons will be that of independent contractor and nothing in this Agreement shall render him an employee, worker, agent or partner of Burlingtons and the Consultant shall not hold himself out as such.

7.2 This Agreement constitutes a contract for the provision of services and not a contract of employment and accordingly the Consultant shall be fully responsible for and shall indemnify Burlingtons for and in respect of:

(a) any income tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the performance of the Services, where the recovery is not prohibited by law. The Consultant shall further indemnify Burlingtons against all reasonable costs, expenses and any penalty, fine or interest incurred or payable by Burlingtons in connection with or in consequence of any such liability, deduction, contribution, assessment or claim; and

(b) any liability arising from any employment-related claim or any claim based on worker status (including reasonable costs and expenses) brought by the Consultant against Burlingtons arising out of or in connection with the provision of the Services.

8. **MISCELLANEOUS**

8.1 This Agreement contains the entire agreement and understanding of the parties and supersedes all prior agreements, understandings or arrangements (both oral and written) relating to the subject matter of the same.

8.2 If a provision of this Agreement is found to be illegal, invalid or unenforceable, then to the extent it is illegal, invalid or unenforceable, that provision will be given no effect and will be treated as though it were not included in this Agreement, but the validity or enforceability of the remaining provisions of this Agreement will not be affected.

8.3 This Agreement may be entered into in any number of counterparts and any party may enter into this Agreement by executing any counterpart. A counterpart constitutes an original of this Agreement and all executed counterparts together have the same effect as if each party had executed the same document.

8.4 The parties do not intend by virtue of this Agreement to confer any rights on any third party pursuant to the provisions of the Contracts (Rights of Third Parties) Act 1999, except that any Group Company shall be entitled to enforce this Agreement.

9. **APPLICABLE LAW AND JURISDICTION**

9.1 Any dispute arising out of or in connection with this contract, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause.

9.2 The number of arbitrators shall be one.

9.3 The seat, or legal place, of arbitration shall be London.

9.4 The language to be used in the arbitral proceedings shall be English.

9.5 The governing law of the contract shall be the substantive law of England & Wales.

Signed by **Burlingtons Legal LLP**)
)
)
)
)
.....)

Signed by **Vikash Kumar Pandey**)
)
)
)
)

DATED 04 SEPTEMBER 2020

VIKASH KUMAR PANDEY

- and -

BURLINGTONS LEGAL LLP

CONSULTANCY AGREEMENT

AGREEMENT IS MADE ON 04 **..... SEPTEMBER 2020**

BETWEEN:

(1) **Vikash Kumar Pandey** of S/O Narmada Pasad Pandey, 272 N Pa Pasan, Pasan, Maharani Laxmi Ward No 12, Kotma Anuppur, Madhya Pradesh - 484336 (**"the Consultant"**); (**"the Consultant"**); and

(2) **Burlingtons Legal LLP** incorporated and registered in England & Wales with company number OC360876 whose registered office is at 5 Stratford Place, London W1C 1AX ("**Burlingtons**").

WHEREAS:

(A) The Consultant is an IT expert and ex-employee of Cyber Root Risk Advisory Private Limited (**"CR"**).

(B) Burlingtons are the English solicitors acting for Mr. Azima who is the Defendant, Counterclaimant and Proposed Appellant in proceedings commenced by Ras Al Khaimah Investment Authority ("**RAKIA**") in the High Court in London under Claim No. HC-2016-002798 (the "**RAKIA Proceedings**"). The RAKIA Proceedings concern, amongst other matters, the hacking of Mr. Azima's emails in around 2015 / 2016 (**"the Hack"**).

(C) The Consultant has agreed to provide assistance to Burlingtons in relation to their investigation into the Hack (**"the Hacking Investigation"**).

(D) It is understood that by assisting Burlingtons with the Hacking Investigation (**"the Purpose"**) the Consultant is risking his reputation within the IT industry and his personal security and that the Consultant may be required to incur substantial costs to ensure that his personal security is protected.

(E) The Consultant has dedicated time, and will need to dedicate further time, to providing information and assistance in connection with the Hacking Investigation. It is agreed that the Consultant will be engaged for the Purpose on the terms set out below.

IT IS AGREED:

1. **INTERPRETATION**

1.1 In this Agreement:

"**Commencement Date**" means 1 August 2020;

"**Confidential Information**" means confidential or secret information relating to Mr. Azima and / or the Hacking Investigation, including, without limitation, the existence and terms of this Agreement and any communications between Burlingtons (and / or its agents and / or advisers) and the Consultant;

"**Services**" means the services described in clause 3.

1.2 In this Agreement, any reference to a statutory provision is a reference to the provision from time to time renumbered, amended, re-enacted or consolidated.

1.3 In this Agreement, unless the context otherwise requires:

(a) references to clauses are to clauses of this Agreement; and

(b) the headings to the clauses are for convenience only and do not affect the Agreement's construction or interpretation.

2. **APPOINTMENT**

2.1 With effect from the Commencement Date, Burlingtons has engaged the Consultant to perform the Services.

3. **SERVICES**

3.1 During his engagement under this Agreement, the Consultant will give information and assistance to Burlingtons and / or its agents in connection with the Hacking Investigation.

3.2 The Consultant acknowledges that this could involve, but is not limited to, assisting in relation to any regulatory or legal process, preparing witness statements and giving evidence in person.

3.3 Without prejudice to the generality of clause 3.1, the Consultant shall make himself available for meetings for up to 30 hours per calendar month (via Zoom or other form of agreed upon video conferring platform), such meetings to take place at Burlington's request upon giving the Consultant at least 3 business days' notice; and

3.4 The Consultant represents, warrants and agrees that:

(a) any information or assistance provided to Burlingtons pursuant to this Agreement will be complete and accurate, and will be given truthfully to the best of the Consultant's knowledge and belief.

(b) he is a former employee of CR and has knowledge of the practices of the company.

(c) The execution, delivery and performance of this agreement will not conflict with:-

(i) Any law or regulation applicable to him; and / or

(ii) Any agreement or instrument binding upon him.

3.5 The Consultant shall indemnify Burlingtons against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred arising out of or in connection with:-

(a) Any breach of the warranties contained in clause 3.4.

(b) Any breach of this agreement.

(c) The enforcement of this agreement.

(d) Any claim made against Burlingtons by a third party arising out of or in connection with the provision of the Services.

3.6 It is agreed that no information or documentation (except as required by an order of a court of competent jurisdiction, or pursuant to any proper order or demand made by any competent authority or body where Burlingtons is under a legal or regulatory obligation to disclose the information and / or documentation) provided by the Consultant pursuant to this Agreement will be used by Burlingtons (on behalf of Mr. Azima) in support of any, action, claim, or prosecution against the Consultant in relation to his liability for the Hack.

4. **REMUNERATION**

4.1 Subject to the terms of this Agreement, Burlingtons shall pay the Consultant the sum of $550 per hour (exclusive of any applicable VAT) in consideration for the provision of the Services for a period of at least 18 months.

4.2 Subject to Burlingtons' prior written approval, Burlingtons shall reimburse all reasonable expenses properly and necessarily incurred by the Consultant in the course of this Agreement, subject to production of receipts or other appropriate evidence of payment.

4.3 The payment referred to at paragraph 4.1 shall include all work undertaken and assistance provided to Burlingtons by the Consultant to the date of this Agreement.

4.4 The period of service referred to at paragraph 4.1 may be extended by written agreement between the parties.

5. **CONFIDENTIAL INFORMATION**

5.1 The Consultant will not, except with the prior written consent of Burlingtons or pursuant to an order of a court of competent jurisdiction, or pursuant to any proper order or demand made by any competent authority or body where the Consultant is under a legal or regulatory obligation to make such disclosure, or to the Consultant's lawyers, auditors or insurers on terms which preserve confidentiality:

(a) disclose or communicate to any person, firm or company;

(b) cause unauthorised disclosure of; or

(c) otherwise make use of,

any Confidential Information that he has or may have acquired in the course of his engagement (whether before, on or after the date of this Agreement) and will use his best endeavours to prevent the unauthorised disclosure or publication of such information. This obligation survives the termination of this Agreement.

5.2 The obligations in clause 5.1 will cease if the relevant Confidential Information comes into the public domain other than through the Consultant's default or negligence.

6. **TERMINATION**

6.1 Upon the termination of this Agreement for whatever reason, the Consultant will deliver up all property and any documents or other information belonging to Burlingtons (and / or to Mr. Azima), including any Confidential Information, whether held electronically or in hard copy, which is in the Consultant's possession or under his control. The Consultant will not retain any copies of any such property, documents or information without written permission from Burlingtons.

6.2 The termination of this Agreement will not affect any of the provisions of this Agreement that are expressed to operate or have effect after its termination (including without limitation clause 5.1) and will not prejudice the exercise of any right or remedy of either party that has accrued prior to termination.

7. **STATUS**

7.1 The relationship of the Consultant to Burlingtons will be that of independent contractor and nothing in this Agreement shall render him an employee, worker, agent or partner of Burlingtons and the Consultant shall not hold himself out as such.

7.2 This Agreement constitutes a contract for the provision of services and not a contract of employment and accordingly the Consultant shall be fully responsible for and shall indemnify Burlingtons for and in respect of:

(a) any income tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the performance of the Services, where the recovery is not prohibited by law. The Consultant shall further indemnify Burlingtons against all reasonable costs, expenses and any penalty, fine or interest incurred or payable by Burlingtons in connection with or in consequence of any such liability, deduction, contribution, assessment or claim; and

(b) any liability arising from any employment-related claim or any claim based on worker status (including reasonable costs and expenses) brought by the Consultant against Burlingtons arising out of or in connection with the provision of the Services.

8. **MISCELLANEOUS**

8.1 This Agreement contains the entire agreement and understanding of the parties and supersedes all prior agreements, understandings or arrangements (both oral and written) relating to the subject matter of the same.

8.2 If a provision of this Agreement is found to be illegal, invalid or unenforceable, then to the extent it is illegal, invalid or unenforceable, that provision will be given no effect and will be treated as though it were not included in this Agreement, but the validity or enforceability of the remaining provisions of this Agreement will not be affected.

8.3 This Agreement may be entered into in any number of counterparts and any party may enter into this Agreement by executing any counterpart. A counterpart constitutes an original of this Agreement and all executed counterparts together have the same effect as if each party had executed the same document.

8.4 The parties do not intend by virtue of this Agreement to confer any rights on any third party pursuant to the provisions of the Contracts (Rights of Third Parties) Act 1999, except that any Group Company shall be entitled to enforce this Agreement.

9. **APPLICABLE LAW AND JURISDICTION**

9.1 Any dispute arising out of or in connection with this contract, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause.

9.2 The number of arbitrators shall be one.

9.3 The seat, or legal place, of arbitration shall be London.

9.4 The language to be used in the arbitral proceedings shall be English.

9.5 The governing law of the contract shall be the substantive law of England & Wales.

Signed by **Burlingtons Legal LLP**)
)
)
)
)

Dominic Holden

Dominic Holden

Partner

04 September 2020

Signed by **Vikash Kumar Pandey**)
)
)
)
)

Exhibit E

On behalf of the Appellant

12th Statement of Dominic Holden

Date: 12 February 2021

CLAIM NO. A3/2020/1271

IN THE COURT OF APPEAL

OF ENGLAND AND WALES

ON APPEAL FROM THE HIGH COURT OF JUSTICE, BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES, BUSINESS LIST (ChD), [2020] EWHC 1327 (Ch) and [2020] EWHC 1686 (Ch)

(Mr Andrew Lenon QC sitting as a Deputy Judge of the High Court)

BETWEEN:

FARHAD AZIMA

Appellant

- and -

RAS AL KHAIMAH INVESTMENT AUTHORITY

Respondent

TWELFTH WITNESS STATEMENT OF

DOMINIC HOLDEN

I, **Dominic Holden**, Partner at Burlingtons Legal LLP ("Burlingtons"), of 5 Stratford Place, London, W1C 1AX **SAY AS FOLLOWS**:

1. I am the same Dominic Holden who provided earlier witness statements in these proceedings. Since Burlingtons' instruction by the Defendants in late June 2019, I have had responsibility (with other fee earners working under my supervision) for the conduct of these proceedings on behalf of Mr. Farhad Azima, the Appellant / Defendant and Counterclaimant. I am authorised by Mr. Azima to make this statement on his

behalf.

2. The facts and matters set out in this statement are within my own knowledge unless otherwise stated, and I believe them to be true. Where I refer to information supplied by others, the source of the information is identified; facts and matters derived from other sources are true to the best of my knowledge and belief.

3. There is now produced and shown to me a bundle of documents marked "Exhibit DPHR12" to which reference will be made in the course of this statement in the form **'[DPHR12/page number]'**.

4. I also make reference to the Witness Statement of Mr. Rey dated 11 February 2021 [**"Rey 1/paragraph number"**] or the Exhibit to Mr. Rey's Statement in the form [Rey 1/JR1/page number]

5. I make this statement in support of Mr. Azima's application to adduce new evidence on appeal, and to rely on a new ground of appeal and a supplementary skeleton argument addressing that new evidence, to be issued on 12 February 2021. The new evidence comprises:-

   (a) Bank statements showing payments amounting to US $1,018,046.39 received by CyberRoot Risk Advisory Private Limited (**"Cyber Root"**) from Vital Management Services Inc. (**"Vital"**) between 28 July 2015 and 22 September 2017.

   (b) LinkedIn profiles and a CV for Ms. Preeti Thapliyal, a CyberRoot employee.

   (c) Witness Statement of Mr. Jonas Rey dated 11 February 2021 and its accompanying exhibit (**"Rey 1"**).

   (d) This witness statement and its exhibit.

   (e) US Complaint filed by Mr. Farhad Azima in the US District Court for the Middle District of North Carolina against Mr. Nicholas Del Rosso (**"Mr. Del Rosso"**) and Vital.

The US Complaint against Mr Del Rosso and Vital

6. On 15 October 2020, Mr. Azima filed a Complaint in North Carolina, USA against Vital and Mr. Del Rosso (**"US Complaint"**) (**DPRH12/523-556**).

7. Mr. Del Rosso is the owner and sole employee of Vital, a company established in North Carolina. Vital purports to provide investigative services (but is not licensed as a private investigator in North Carolina).

8. Mr. Del Rosso appeared as one of RAKIA's witnesses at trial having also filed a witness statement dated 21 June 2019. Mr Del Rosso's evidence was that he played only a

limited role in RAKIA's discovery of Mr. Azima's hacked data. He stated that (Mr Del Rosso's witness statement, paras 4-6):

> *"4. In August 2014, Vital was engaged by Dechert LLP to investigate assets potentially stolen from the Government of Ras Al Khaimah ("RAK"). Pursuant to its engagement VMS examined potential frauds committed by, amongst others, Khater Massaad. I took my instructions from Dechert LLP, and had limited direct contact with Jamie Buchanan and other representative of the RAK government. I worked previously with other lawyers then at Dechert LLP on unrelated matters involving suspected fraud.*
>
> *5. In early August 2016, I received a telephone call from Neil Gerrard of Dechert. During that call, Neil told me that Stuart Page had identified two links on the internet which appeared to contain data relating to Farhad Azima, an associate of Khater Massaad. I do not know Stuart Page but I had heard of him because he works in a similar industry to me.*
>
> *6. When Neil and I spoke, he asked if VMS* [Vital] *could assist in retrieving the data that had been found, or if VMS could engage a suitable forensic data specialist to do so. He then dictated to me over the phone the details of the two links where the information could be found. I do recall Neil warned me that the material could contain viruses…"*

9. Mr Del Rosso goes on to state that he then proceeded to engage Northern Technology, Inc. to download the data.

10. The crux of the US Complaint is that Mr. Del Rosso / Vital were in fact instructed by Mr Neil Gerrard of Dechert LLP, acting on RAKIA's behalf, to hack Mr. Azima's emails and disseminate Mr. Azima's confidential data. Mr. Del Rosso / Vital hired an Indian firm, Cyber Root, which was assisted by BellTrox Info Tech Services (**"BellTrox"**). That assistance included BellTrox providing CyberRoot with access to its existing infrastructure to carry out the hack (see para 16 of the US Complaint (**DPRH12/529**)). Cyber Root and BellTrox are "hack-for-hire" firms.

11. After successfully gaining persistent access to Mr. Azima's data, Cyber Root arranged for the data to be published online through the peer-to-peer file sharing website, BitTorrent. Vital paid more than $1 million to Cyber Root for this work.

12. As part of the US Complaint, Mr. Azima filed a Motion for early discovery, including of Vital's banking records. Vital / Mr. Del Rosso strongly resisted providing any early discovery, and the Motion was dismissed. Vital / Mr. Del Rosso in turn filed a Motion

to Dismiss, and Mr. Azima has filed a further Motion for early discovery (**DPRH12/1-6**). At the time of writing, the US Court is yet to rule on these two Motions.

Mr. Azima's post-trial Hacking Investigation

13. The US Complaint is based on evidence and information that emerged from further investigations into the hacking of his emails following the handing down of Deputy Judge Lenon QC's Judgment dated on 22 May 2020 (**"the Judgment"**).

14. Without any waiver of privilege, Mr. Jonas Rey of Athena Intelligence & Risk Management Sarl has undertaken various investigations on the instructions of Burlingtons. Mr Rey's witness statement dated 11 February 2021 sets out information that he has obtained regarding Cyber Root.

15. The Court will note that one of the sources who provided their co-operation to Mr. Rey, wishes to remain anonymous under fear of retribution from Cyber Root (Rey 1/paragraph 4). Further, those individuals who have come forward and spoken openly to Mr. Rey have since been contacted by Cyber Root and directed not to cooperate, with warnings of serious consequences should they do so (Rey 1/paragraphs 40-43). Those individuals have since refused to provide a statement for use in legal proceedings or to provide any further information.

16. In the circumstances, and without any waiver of privilege, Mr. Azima has until now refrained from bringing this application to adduce evidence relating to the matters in the US complaint in view of the rules governing the admission of new evidence on appeal. However, compelling corroborating evidence has now emerged which has changed the position.

Cyber Root's Bank Statements

17. The position altered significantly in light of developments in the last week. On Friday, 5 February 2021, Stokoe Partnership Solicitors (**"Stokoe"**) filed an application in North Carolina in relation to Mr. Del Rosso and Vital. This filing is separate from Mr. Azima's case in North Carolina. The filing has been made available to the public on the PACER records system of US Federal Courts; a zip older of the documents published on PACER is at **DPRH12/6-656**.

18. Stokoe's filing in the US Court seeks an order under 28 USC §1782 to obtain evidence from Mr. Del Rosso and Vital in connection with Stokoe's complaint (explained below) that attempts were made to obtain Stokoe's confidential information without its authorisation.

19. The filing includes a Declaration dated 5 February 2021 made by Mr. Bambos Tsiattalou (**"Mr. Tsiattalou"**), an English solicitor and a partner in Stokoe (**"the Declaration"**) **DPH12/61-79**. The Declaration exhibits bank statements for Cyber

Root, and it is these bank statements that Mr. Azima seeks to rely on (along with other evidence).

The Al Sadeq and Stokoe proceedings

20. By way of background to the US filing, Mr. Tsiattalou and Stokoe are currently representing Mr. Karam Al Sadeq in his claim before the English High Court (QB-2020-000322) against Dechert LLP, Mr. Neil Gerrard, Mr. David Hughes and Ms. Caroline Black (who are or were partners at Dechert) concerning Mr Al Sadeq's complaint of misconduct and human rights abuses committed against him in connection with RAKIA's investigation of alleged frauds (**"the Al Sadeq Proceedings"**). As noted above, Mr Gerrard and Dechert have also acted for RAKIA in respect of its investigation into Mr. Azima, as has Mr. Hughes. The allegations in the Al Sadeq Proceedings are summarised in paragraph 9 of the Al Sadeq Claim (**DPRH12/82-83**).

21. Stokoe have also brought their own proceedings in the High Court against various parties, complaining of attempts to access Stokoe's confidential information, including banking information (described as the *"Robinson"* and *"Grayson"* Proceedings, and collectively as the **"Stokoe Hacking Claims"** – *see* paragraph 1 of the Declaration). The background to the Stokoe Hacking Claims is summarised at paragraphs 13-15 of the Declaration (**DPRH/66-67**).

22. Mr Tsiattalou explains that since the commencement of the Al Sadeq Proceedings, he, his firm, Mr Al Sadeq's counsel and others involved in those proceedings on Mr Al Sadeq's side have been targeted by phishing emails, and that Stokoe's IT systems have been attacked (**Declaration, paras 43-45**). Mr Tsiattalou explains that this is part of an attempt to disrupt the representation of Mr Al Sadeq in his claim. Stokoe has brought proceedings against several different individuals and entities believed to be involved in the hacking (**Declaration, paras 33-42**). Several of those individuals have made admissions and named others involved; one such person named as providing instructions to obtain the confidential information is a Mr Grayson (discussed further below). These developments were summarised by Mr Justice William Davis in *Stokoe Partnership Solicitors v Robinson* [2020] EWHC 3312 (QB) at paras 4-9.

23. As Mr Tsiattalou notes, the claim brought by Mr Al Sadeq is related to these proceedings (**Declaration, para 17**). Part of the factual background to the Azima proceedings overlaps with the Al Sadeq Proceedings. Paragraphs 2 and 30 of Deputy Judge Lenon QC's Judgment records that the Azima Proceedings involved an investigation conducted by RAKIA from around late 2014 into RAKIA's former Chief Executive Officer, Dr. Massaad (**"Massaad Investigation"**). As part of the Massaad investigation, Mr. Al Sadeq, who was formerly employed by RAKIA, was arrested by the RAK authorities. After a lengthy period of detention without charge, he was ultimately charged and convicted by a RAK court. While detained, Mr Al Sadeq was repeatedly interrogated by Mr Gerrard and other Dechert solicitors. I understand that Mr Al Sadeq maintains that his conviction was secured by false evidence obtained through torture. The question of whether human rights abuses had been committed

against Mr. Al Sadeq became an issue in the Azima proceedings after Mr. Azima took steps to draw attention to these abuses (*see* paragraphs 201-202 of the Judgment).

The Cyber Root bank statements

24. Paragraph 32 of the supporting Declaration states as follows:

> *"On October 15, 2020, Mr. Azima filed a complaint in this District against Del Rosso and Vital Management, alleging, inter alia, that Del Rosso through Vital Management oversaw and directed the hacking of Mr. Azima's personal information by utilizing the services of CyberRoot Risk Advisory Private Limited ("CyberRoot") and BellTroX Info Tech Services ("BellTroX") which are well known hack-for-hire organizations located in India. A copy of the complaint, filed by Mr. Azima, is annexed as* ***Exhibit F*** *hereto. Mr. Azima alleges that Del Rosso paid CyberRoot more than $1 million to hack Mr. Azima's personal and confidential information and post that information online. Ex. F, p. 7-9. A whistleblower who is employed by CyberRoot and who has legitimate access to the company's bank account has provided copies of what the Applicants believe are CyberRoot's bank account statements with Kotak Mahindra Bank. A copy of CyberRoot's bank account statements reflecting payments made by Vital Management to CyberRoot is annexed as* ***Exhibit G*** *hereto in redacted form to eliminate references to entities other than Vital Management and to eliminate account numbers."*

25. Exhibit G comprises images taken of bank statements for Cyber Root (*'Bank Statements'*), with headings indicating that the Bank Statements were issued by Kotak Mahindra Bank, from a branch in India.

26. The Bank Statements record that substantial sums ($1,018,046.39) were received by Cyber Root from Vital. A table (prepared by Burlingtons) of the payments listed by the Bank Statements is at **DPRH12/657-658**.

27. The Bank Statements clearly corroborate Mr Azima's US complaint against Mr Del Rosso and Vital, and his claim in these proceedings that RAKIA is responsible for the hacking. In particular:

- Between July 2015 and September 2017, Cyber Root received amounts totalling $1,018,046.39 from Vital.

- Substantial sums were paid at times coinciding with the placing of the tranches of Mr Azima's data on the BitTorrent sites. Some $132,483.34 was received in

two payments in late July and early August 2016 (entries 10 and 11), which is close in time to a critical meeting between Mr Gerrard, Mr Buchanan and Mr Azima (which took place on 16 July 2016), and to the posting of the first tranche of Mr Azima's data on around 4 August 2016.

- A further $14,991.67 was received on 26 August 2016 (entry 12), around the same time as the second tranche of data (which was much smaller than the first and third tranches) on around 30 August 2016.

- A further $76,491.67 was received (entries 13-16) immediately before and after the third tranche of data appeared, on around 8 September 2016. Further payments followed.

28. There is clear evidence that Cyber Root is a 'hack-for-hire' firm with links to BellTrox. I note for example that:

a. Source 1 has confirmed that Cyber Root is a 'hack for hire firm' to Mr. Rey (**Rey 1 / paragraph 10**).

b. Vikash Pandey, a former Cyber Root employee introduced to Mr Rey by Source 1, has admitted to Mr. Rey that he and four others had directly worked on the hack of Mr. Azima while at Cyber Root (**Rey 1/paragraph 15**).

c. A current employee of Cyber Root, Ms. Preeti Thapliyal, was previously employed by BellTrox[1] (**Rey1/paragraph 44.4**). BellTrox has been publicly implicated in hacking. On 11 February 2015, the founder and owner of BellTrox, Sumit Gupta, was indicted by the United States Department of Justice in the Northern District of California for hacking. Mr. Gupta remains at large. According to a June 9, 2020 press report by Thomson Reuters, BellTroX was involved in "*one of the largest spy-for-hire operations ever exposed*," helping clients spy on more than 10,000 email accounts over a period of seven years.[2]

d. Preeti Thapliyal has stated in her Linked In profile (**Rey1/JR181 and 82**) that while at BellTrox she, "*Worked on Custom Build Phishing Campaigns*

[1] Ms. Thapliyal's LinkedIn profile as published on 28 July 2020 is at **Rey1/JR1/81** and as published on 8 February 2021 is at **Rey1/JR1/82**
[2] See https://www.reuters.com/article/us-india-cyber-mercenaries-exclusive/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUKKBN23G1GQ?edition-redirect=uk (**Rey1/JR1/2-18**)

Framework", and "*Created undetectable phishing Payloads*". Prior to working at BellTrox, she stated that she "*Worked on a project of Hardware hacking using Rfid and Arduino*".

e. I note that the first screen print Mr. Rey took of Ms. Thapliyal's Linked In Profile on 28 July 2020 stated that she had worked for Cyber Root, whereas the screen print taken by Mr. Rey on 8 February 2021 (following the commencement of the proceedings in North Carolina) shows that Ms. Thapliyal has removed the reference to Cyber Root and replaced it with the word "confidential". The text is otherwise identical, however (**Rey1/paragraph 44.6**).

f. At **Rey/JR1/83-84** is a December 2018 redacted copy of Ms. Thapliyal's Curriculum Vitae[3] which she provided to Mr. Rey (**Rey 1 / paragraph 44.7**). The Court will note that she states in the section dealing with her work with Belltrox that she:

"Worked on Custom Build Phishing Campaign Framework" and
"Created undetectable phishing Payloads"

g. She further confirms that (as at the date of that CV) she was working for Cyber Root.

29. Source 1 has also confirmed to Mr. Rey that they understood Cyber Root to have been paid more than $1 million for these tasks, and that Cyber Root did this work for RAKIA (**Rey 1 / paragraph 13**).

30. In my considered view, the Bank Statements, and the other information summarised above concerning Cyber Root, provide compelling support for the conclusion that Cyber Root (conceivably amongst others) carried out a successful hacking attack on Mr Azima and then assisted with the dissemination of his data on the internet, for which Cyber Root was instructed and paid by Vital.

31. The connection to RAKIA (and RAKIA's culpability) clearly follows because Mr Del Rosso has admitted that he was retained by Mr Gerrard on behalf of Dechert to provide services to RAKIA (Mr Del Rosso's Statement, paragraph 4). Mr. Gerrard has admitted this as well (Witness Statement of Mr Gerrard dated 24 June 2019, paragraph 19

[3] The CV has been redacted to remove Ms. Thapliyal's personal data (contact number, email ID, address, Pincode, marital status, father's name and mother's name).

(**DPRH12/659-664**). Indeed, as explained below, RAKIA has now (in their letter to Burlingtons dated 11 February 2021) re-affirmed that Mr. Del Rosso and Vital were acting on its behalf, instructed by Dechert.

RAKIA's response to this evidence

32. By a letter dated 23 October 2021 (**DPRH12/665-666**), Burlingtons put RAKIA on notice of the US Complaint against Mr Del Rosso and Vital and provided their solicitors with a copy of the complaint itself. Burlingtons invited RAKIA to respond and to address the following specific questions in particular:-

- Who directed the work of Mr. Del Rosso for the benefit of RAKIA?
- What fees and/or expenses were charged by Mr Del Rosso and/or Vital for the services provided by them or by others procured or appointed through or by them?
- What fees and expenses were paid by Dechert LLP (or any entity connected to it) or by RAKIA directly?
- What payments were made directly or indirectly by Mr Del Rosso/Vital to Cyber Root, or another Indian company named in the Complaint as assisting Cyber Root, Bell Trox, or any entity or individual connected with them in regard to services relevant to Mr Del Rosso/ Vital's engagement by Dechert/RAKIA otherwise for the benefit of RAKIA; and in return for what services?
- On whose instructions Mr Del Rosso/Vital made those payments?
- What knowledge did Mr Gerrard and/or Mr Hughes have about these matters?

33. In their reply on 29 October 2020 (**DPRH12/667-668**), Stewarts refused to provide answers to these questions.

34. On 8 February 2021, Burlingtons sent a further letter to Stewarts providing them with a complete copy of the §1782 application filed by Stokoe and publicly available

information indicating that Cyber Root is a 'hack-for-hire' firm, and inviting RAKIA again to answer these questions by noon on 11 February 2021 (**DPRH12/669-672**).

35. RAKIA responded to this letter on 11 February 2021 (**DPRH12/673-675**). Its response by implication accepts certain key points put to it but otherwise fails to engage with the case against it that this new evidence points to, and is overall highly evasive. In particular:

(a) RAKIA confirmed that Mr. Del Rosso acted for RAKIA on instructions from Dechert.

(b) RAKIA's letter does not deny that any payments were made by Vital to Cyber Root on its behalf. Rather, it includes the heavily qualified statement that, "*No payments were made to CyberRoot or Bell Trox by Mr Del Rosso/VMS in relation to any matters undertaken for RAKIA in relation to Mr Azima*". This statement obviously falls short of a denial across the board of any payments to Cyber Root or Bell Trox. It would be expected that if there had been no such payments, RAKIA would be eager to offer that denial.

(c) Presumably, RAKIA realises that there will be a documentary record of payments by Vital to Cyber Root, held by third parties (the banks in question). In the face of the bank statements and the lack of any general denial by RAKIA, it may be inferred that the bank statements accurately record that very substantial payments were made by Vital to Cyber Root, presumably on RAKIA's behalf.

(d) Having (at the very least) left open the possibility that payments were made to Cyber Root and/or Bell Trox by RAKIA (through Vital or otherwise), it is then striking that RAKIA does not engage at all with the evidence pointing to those firms' involvement in hacking, including the statements by a Cyber Root employee.

36. Overall, RAKIA's response provides no meaningful answer to the case now put to it. If anything, its response heightens suspicion.

Application to admit new evidence

37. With the Court's permission, Mr Azima will seek to develop his application to admit this new evidence at the time the Court may direct. In summary, it is submitted that the

test for the admission of new evidence on an appeal is satisfied for the following reasons.

38. **Unavailability of the evidence at trial -** The information and evidence that Mr Azima seeks to adduce only came into his possession following the trial. Mr Azima had made concerted efforts to investigate the hacking prior to trial but this information had not come to light: the information had been concealed by the parties involved in the hacking. I would respectfully suggest that Mr Azima could not reasonably be expected to have obtained this information by the time of trial.

39. **Credibility of the evidence -** It is submitted that this evidence is also "apparently credible" (at least). It is largely based on statements and admissions by the individuals at CyberRoot involved in hacking (which are credible since they are admissions against those individuals' interests), and on contemporaneous business records (the Bank Statements).

40. **Conclusions to be drawn from the evidence -** For the reasons set out above, I respectfully submit that the evidence is cogent and so would have the required "important influence" on the result of the case.

    (a) A range of information – including publicly available information and admissions by individuals at CyberRoot – shows that it is a 'hack for hire' firm.

    (b) The Bank Statements make clear that Vital made significant payments to CyberRoot at the times when the fruits of the hacking were placed online.

    (c) Admissions made to Mr Rey confirm these facts.

    (d) Vital is in turn RAKIA's agent, instructed by Mr Gerrard of Dechert (also acting for RAKIA).

    (e) This evidence – certainly when put together with the other evidence and findings in the case pointing to RAKIA's responsibility for the hacking, would, I submit, be sufficiently cogent to have an "important influence" on the outcome of the case.

The relationship between these facts and the facts established at trial

41. It is of course of the essence of unlawful hacking that is executed covertly. Mr Azima has been forced to piece what happened together by ongoing investigations and in the face of obstruction, denial and obfuscation.

42. For all the reasons canvassed in the appeal, it is overwhelmingly probable that Mr Page, acting for RAKIA, was party to the hacking, the dissemination of the data and the cover-up of its provenance. The evidence canvassed above shows that Mr Del Rosso and Cyber Root were also key players. Indeed, it may be that others were also involved, but Mr Azima does not yet have evidence meeting the requisite standard to prove that involvement (but explains one further line of inquiry below for the Court's information). RAKIA, as the judge found, has yet to provide a truthful and frank account of how it came to possess the hacked data; and the overwhelming inference is that it used a range of parties and means to do so, including at least Mr Page and Mr Del Rosso.

43. One other line of inquiry is as to the involvement of a Mr Grayson and his investigations firm, GPW + Co Ltd. (**"GPW"**). Mr Azima has reason to believe that Mr Grayson and/or GPW were engaged by RAKIA in relation to RAKIA's investigation into him. This is notable for several reasons:

    (a) In the Stokoe Hacking Claim, Mr Grayson has been credibly identified as providing instructions to other persons to obtain Stokoe's confidential information. The identification has been made by another person who has admitted attempting to obtain the information.[4] That appears to confirm that Mr Grayson was prepared to engage in unlawful conduct of that kind.

    (b) None of RAKIA's pleadings or witnesses alluded to Mr Grayson at all, as having any involvement of any kind in the matters at issue.

    (c) Prior to trial, RAKIA was ordered to provide a response to a CPR Part 18 request (Request 9(d)) requiring it to, "*provide the names of each*

[4] The position is set out in the judgement of Mr Justice William Davis in *Stokoe Partnership Solicitors v Robinson and others* [2020] EWHC 3312 (QB) (paragraphs 4-9) (**DPRH12/676-692**). Stokoe discovered that a Mr Robinson had been attempting to obtain its confidential information, including banking information. After Stokoe brought proceedings against Mr Robinson and applied for Norwich Pharmacal relief, he was ordered to swear an affidavit in regard to his instructions, in which he then stated that, *"His instructions came from Patrick Grayson who was a private investigator and by whom Mr Robinson had been instructed in the past."* He provided various documents confirming that he had met and communicated with Mr Grayson from January 2020 onwards.

investigations and public relations entity (in addition to Bell Pottinger) engaged by RAKIA, the individuals within those entities who carried out the engagement and the location of those individuals." RAKIA's response did not refer to Mr Grayson or GPW (**DPRH12/693-716**).

(d) For the purposes of disclosure, RAKIA was also ordered to seek documents from all of its agents. RAKIA's disclosure statement (**DPRH12/717-739**) referred to various other agents as having been asked to provide documents, but not to Mr Grayson or GPW.

44. Burlingtons wrote to RAKIA on 29 January 2021 to ask whether Mr Grayson or GPW was engaged by it (**DPRH12/740-741**). Despite being chased, RAKIA provided a response only today (2 weeks after Burlingtons' letter) (**DPRH12/742-743**). Its response is again highly evasive:

(a) RAKIA does not deny that Mr Grayson and/or GPW were engaged by RAKIA. It offers no explanation as to what Mr Grayson and/or GPW was in fact engaged to do. It offers no response to the allegations relating to Mr Grayson in the Stokoe litigation.

(b) RAKIA suggests that the Part 18 request was essentially focussed on identifying agents who were monitoring the press and media regarding the dispute. This is a highly artificial and strained reading of the Part 18 response, which requires RAKIA to identify the "investigations and public relations entities" who carried out "the engagement". The "engagement" was defined in the pleadings as follows: "

> *"In connection with this dispute, RAKIA engaged investigators and public relations consultants (including Bell Pottinger). In the course of these engagements, RAKIA's agents monitored the press, internet and other media for reports regarding Ras Al Khaimah and the individuals involved on both sides of the dispute."*

(c) The engagement was not limited to carrying out "monitoring"; the monitoring referred to was simply described as something done in the course of "the engagement".

(d) RAKIA suggests that no request for documents was made to Mr Grayson and GPW because it was believed that they held no relevant documents. I would however note that a number of RAKIA's agents in fact had no documents at all but that requests were still made of them (including Mr Page).

45. RAKIA's response thus raises further suspicion. Mr. Azima will continue to investigate these matters and will be prepared to address the Court further on them as appropriate.

Conclusion

46. The Court is respectfully asked to allow the new evidence to be adduced, and to have regard to it in the determination of the appeal.

Statement of truth

I believe that the facts stated in this witness statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed: Dominic Holden

Name: Dominic Holden

Position: Partner, Burlingtons Legal LLP

Dated: 12 February 2021

Filed on behalf of the Appellant

Twelfth Witness Statement of Dominic Holden

Date: February 2021

Appeal No.: A3/2020/1271

IN THE COURT OF APPEAL

(CIVIL DIVISION)

ON APPEAL FROM THE HIGH COURT OF JUSTICE, BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES, BUSINESS LIST [2020] EWHC 1327 (Ch) and [2020] EWHC 1686 (Ch) (Mr Andrew Lenon QC sitting as a Deputy Judge of the High Court)

BETWEEN:

FARHAD AZIMA

Appellant

- and -

RAS AL KHAIMAH INVESTMENT AUTHORITY

Respondent

TWELFTH WITNESS STATEMENT OF DOMINIC HOLDEN

Burlingtons Legal LLP
5 Stratford Place
London
W1C 1AX
DX 82986 MAYFAIR
DH/AZI0003.2
Solicitors for the Defendant / Appellant / Counterclaimant

On behalf of: The Appellant
Witness: Jonas Rey
1st witness statement
Exhibit JR1
Date: 11 February 2021

IN THE COURT OF APPEAL **Appeal No: A3/2020/1271**

(CIVIL DIVISION)

ON APPEAL FROM THE HIGH COURT OF JUSTICE, BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES, BUSINESS LIST (ChD), [2020] EWHC 1327 (Ch) and [2020] EWHC 1686 (Ch) (Mr Andrew Lenon QC sitting as a Deputy Judge of the High Court)

B E T W E E N:

FARHAD AZIMA

Appellant

-and-

RAS AL KHAIMAH INVESTMENT AUTHORITY

Respondent

WITNESS STATEMENT OF
JONAS REY

I, **JONAS REY**, of Chemin du Plat de Valencon 10, 3978 Flanthey, Switzerland state as follows:

1. I am the CEO and founder of Athena Intelligence & Risk Management Sarl (**"Athena Intelligence"**), a private intelligence firm.

2. I specialize in investigating financial and cyber-crimes. Before founding Athena Intelligence, I was employed by Diligence, a multinational private intelligence firm, from 2012 until 2019. I have a Masters degree in international relations with a focus on Internet governance from the University of Lucerne, Switzerland. Athena Intelligence is duly accredited with the Federal Department of Foreign Affairs of Switzerland as a provider of intelligence services. Furthermore, Athena Intelligence is a founding member of ASPIRE, the Swiss Association for Professionals of Business Intelligence. A full copy of my Curriculum Vitae can be found at **JR1/1**.

3. The facts and matters set out in this statement are within my own knowledge unless otherwise stated, and I believe them to be true. Where I refer to information from other sources, the source of the information is identified; facts and matters derived from other sources are true to the best of my knowledge and belief.

4. In this statement I refer to a number of 'Sources' who have assisted me with my investigation. I have identified these sources save for Source 1 who I have agreed should remain anonymous for the purposes of this statement because they fear that should their identity be exposed their personal security may be compromised.

5. I make this Statement in relation to Mr. Farhad Azima's (**"Mr. Azima's"**) allegation that the Ras Al Khaimah Investment Authority ("**RAKIA**") was responsible for the hacking of his emails and personal data.

6. There is now produced and shown to me in a bundle of documents marked **"JR1"** to which reference is made in the course of this statement in the form **'[JR1/[page number]'.**

7. In places in this statement, I refer to various communications connected with litigation. For the avoidance of doubt, to the extent that I make any such references, these are not intended to waive, and should not be regarded as a waiver of, privilege (which is in any event not mine to waive).

My Investigations and Sources

8. On 6 July 2020, I was instructed by Burlingtons Legal LLP, acting on behalf of their client, Mr Azima, to investigate whether the Indian firm BellTroX Info Tech Services (**"BellTrox"**) had been involved in the hack of Mr Azima's emails and data (**"the Hacking Investigation"**). This instruction followed the trial in the proceedings between RAKIA and Mr Azima, and reports in the press regarding BellTrox alleging that it was a "hack-for-hire group"[1].

9. As part of this investigation, I contacted multiple individuals in India, including a cybersecurity expert whom I anticipated might be able to point out in which directions I should investigate further regarding such matters (**"Source 1"**).

[1] https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation (**JR1/2-18**) and https://uk.reuters.com/article/us-india-cyber-mercenaries-exclusive/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUKKBN23G1GQ (**JR1/19-24**)

10. I asked Source 1 whether they had heard that BellTrox had been hired to hack the emails of Mr. Azima that were subsequently released on the internet through a peer-to-peer file sharing site, called BitTorrent[2]. Source 1 informed me that it was in fact Cyber Root Risk Advisory Private Limited (**"Cyber Root"**) that had been hired to carry out the hacking, although as I explain below, BellTrox also had a role. Source 1 explained that Cyber Root is another 'hack for hire' firm similar in nature to BellTrox.

11. Source 1 further explained that multiple firms in India had also been approached by Mr. Stuart Page to carry out hacking of Mr. Azima as early as October 2014.

12. Source 1 explained however that they were confident in their information as they personally knew a number of former employees of Cyber Root, who were in charge of the social engineering work for several of Cyber Root's cases.[3] Source 1 subsequently suggested that I reach out to Rajat Shirish **("Rajat"),** a former employee of Cyber Root. Rajat Shirish subsequently mentioned and introduced me to a former employee of Cyber Root, a Mr. Vikash Kumar Pandey (**"Vikash"**). Vikash had trained employees of Cyber Root in the methods of undertaking phishing[4] and social engineering campaigns. I understand that Vikash was initially a freelance subcontractor to Cyber Root from 2013. In 2016, he became a full employee of Cyber Root.

13. Source 1 told me that Cyber Root had been paid over $1 million for the work, and that he understood that Cyber Root did this work for RAKIA.

14. I then proceeded to have direct communications with Vikash. Vikash's main language was Hindi but his written English was passable and he used written English on his work on a day-to-day basis. Most of my oral discussions with Vikash were via Rajat and Source 1. I would generally ask questions in English and Vikash would answer in Hindi, which Rajat and Source 1 were able to interpret. On occasion, Rajat or Source 1 would also interpret my questions for

---

[2] BitTorrent is a website which allows for searching of torrent files. Torrent files are peer to peer files that are usually used to exchange large amounts of data. BitTorrent and Piratebay are the most well- known torrent search engines.

[3] Social engineering is the act of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information or access your computer to secretly install malicious software that will give them access to your passwords and bank information, as well as giving them control over your computer. (source: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering). It is called social engineering as this type of attack always has a human interaction aspect to it. It usually takes the format of email exchanges between the victim and the attackers.

[4] A phishing attack is an attack vector used by hackers in order to harvest the login credentials of their target, It usually involves sending a fake email which looks like a real password reset email from various internet service providers. It invites the victim to enter their current login and passwords. The attacker will then receive this information and use it for their own benefits. It is one of the most common attack by hackers.

Vikash (sometimes by repeating the question in English but with a strong Indian accent). Those discussions were through Zoom calls at which Vikash, Rajat, Source 1 and I were all present. I also obtained information from Vikash through written messages passing through Rajat and Source 1.[5] On the Zoom calls I would then ask Vikash to confirm some of the information obtained through written messages.

Methods Adopted by Cyber Root

15. Vikash explained to me that he and four of his colleagues (including Mr. Vibhor Sharma – the CEO of Cyber Root – "**Mr Sharma**") had directly worked on the hack of Mr. Azima and that Cyber Root's instructions were provided by Mr. Nicholas Del Rosso (**"Mr. Del Rosso"**) one of the directors of a US-based company, Vital Management Services Inc. ("**Vital**").

16. From my communications with Vikash (including information provided by Vikash via Source 1 and Rajat as explained above), I understand that a team of Cyber Root employees in addition to Vikash were engaged in attempting to hack Mr. Azima's data and that different members of the team worked on this project at different times. I understand from Vikash that he began working on the project in approximately June or July 2015. From my discussions with Vikash, I believe that others were working on it earlier but I do not know any of the details. Vikash told me that the team at Cyber Root were initially unsuccessful.

17. Cyber Root were also tasked by Mr. Del Rosso with hacking Dr. Khater Massaad (**"Dr. Massaad"**) at around the same time in 2015. They had successfully hacked Dr. Massaad by July 2015 after they compromised Forsan Ceramics (**"Forsan"**), a key company of Dr. Massaad through a successful phishing attack.

18. They then attempted to compromise Mr. Azima by creating spoofed emails[6] that would appear to Mr. Azima to have been sent to him by his friends and relatives. However, Vikash informed me that despite these efforts they were not successful. In March 2016, Cyber Root sent Mr. Azima a phishing gmail password reset email which Mr. Azima ultimately accepted. Using this technique, they were able to compromise Mr. Azima's email account in around the end of March / early April 2016 and gained access to Mr. Azima's emails.

---

[5] As is common in corporate intelligence gathering, the written communications I had with Vikash (including via Rajat and Source 1) were 'disappearing' messages; ie, messages that would appear on my device but would then be automatically deleted by the communication app.

[6] Spoofed emails are emails that appear to come from a legitimate source (such as Google or Facebook or other online services), but are in fact fake emails coming from hackers and various attackers.

19. Once they compromised Mr. Azima's emails, and upon the request of Mr. Del Rosso, Cyber Root set up methods to monitor Mr. Azima's ongoing emails. I understand from Vikash that the means used to share emails with their client was through WeTransfer[7] links.

20. Vikash was able to expand on those points in discussing them with me as he is the developer that was responsible for developing the phishing infrastructure of Cyber Root. Through his work, he was directly responsible for designing the backbone infrastructure that was then used to conduct phishing and social engineering attacks on Mr. Azima.

21. Source 1 explained to me that $1 million is considered to be a high price for a hack of this nature. Vikash explained that the high price was justified because of the ongoing monitoring work. This monitoring increased the risk profile of the work as continued monitoring raises the chances of being detected.

22. Cyber Root were also engaged to disseminate the hacked material once it had been obtained which added to the cost of the work (I deal with this further below in relation to the way in which the hacked material was disseminated).

23. Vikash explained that Cyber Root had used AirVPN a popular Virtual Private Network (**"VPN"**) which obfuscates one's IP's address[8] for anonymity.

24. Phishing infrastructure is usually quite complex as the hacker would need multiple servers to conduct this effectively. Vikash explained that at the time of the hack, in 2015 and 2016, Cyber Root was initially lacking hacking infrastructure. As such, they had asked BellTrox (and Sumit Gupta- the founder and director of BellTrox - specifically), if Cyber Root could piggyback on BellTrox's infrastructure. Vikash explained that in the initial period of the hacking attack, Cyber Root used part of BellTrox's infrastructure to compromise Mr. Azima's emails. He explained that the phishing server[9] of BellTrox was used by Cyber Root to target Farhad Azima. The phishing was conducted using various online services, including EMKEI.CZ and ReadNotify. As I explain above, Vikash also developed hacking infrastructure for Cyber Root, which was then used subsequently.

---

[7] Wetransfer is a platform to share large files online. The free version allows for the file to remain available to download for 30 days. The pro version has a customized timeframe where the file remains online.

[8] An IP address is a unique string of characters that identifies each computer using the Internet Protocol to communicate over a network. IPs can be obfuscated by routing Internet traffic through a third party (the VPN).

[9] A Phishing server is a server which is used to replicate web-pages of real internet services which invites victims to enter credentials.

Cyber Root's Dissemination of Mr Azima's Data

25. Vikash explained that Cyber Root was instructed to assist Vital by disseminating Mr Azima's hacked data online.

26. For this purpose, Mr. Sharma (Cyber Root's director) established a 'torrent' on Piratebay[10].

27. Vikash confirmed that Mr. Sharma set up the Piratebay account in the name of "an_james" which he used to upload the torrent. The same Mr. Sharma, according to Vikash, also manages the email handled "an_james@protonmail.ch", which has been used to create a professional WeTransfer account and which he has used to post the links to the torrent(s) on numerous blogs controlled by Cyber Root (see below).

28. Torrent links were used as the data would only then be accessible if a 'seeder' was available[11]. Accordingly, by using a seeder they controlled, they had control of when the data was publicly available. If they closed down the seeder (e.g. the seeder was made to be offline), no one else would be able to download the data.

29. He further explained that various web pages were created in early August 2016 with links to various torrent links. This was done in a way to mimic a genuine whistleblower campaign in similar fashion to offshore leaks like the Panama Papers. This would allow Vital and / or other entities working with Vital to claim that they had found those documents in the public domain and were thus perfectly allowed to use them in RAKIA's case against Mr. Azima.

30. The websites were created by Cyber Root employees and links to those page are still visible today on this page: http://www.bookmark4you.com/tag/farhad-azima-fraud (**JR1/25-26**)[12].

31. Further research I have conducted about the websites identified in bookmark4you, shows that some of the pages created, such as https://farhadazimascams.blogspot.com/2016/08/farhad-azima-and-his-associate-ray.html also contain an alternative link to the Bit Torrent and also

---

[10] Piratebay is a search engine which allows the user to find a torrent. Piratebay was used to publish the link to the hacked material of Mr. Azima.

[11] A torrent 'seeder' is a user who owns the file being made available online through the torrent system. The torrent then replicates the content of the file on the seeder's computer to other users via the torrent system. Without a seeder, a file cannot be downloaded.

[12] Bookmark4you bookmarks and backlinks webpages which is used for search engine optimization purposes. In order to rank websites and pages high in traditional search engines such as Google, one needs to build the legitimacy of a website. By using Bookmark4you, individuals can artificially increase the legitimacy of various webpages in order for Google to rank them higher. Such search engine optimization techniques work best when used on multiple platforms, such as Bookmark4you, Reddit and other blogs.

references to a number of WeTransfer links. This page also contains two further comments made in 25 May 2018 and 11 June 2018, which then link to the Wordpress website https://exposedfarhadazima.wordpress.com/ (**JR1/27-28**)

32. All those bookmarks were posted by the same user "Aabid236", and a history of his posts can be found here: http://www.bookmark4you.com/user/2269909-aabid236 (**JR1/29-30**).

33. The same username was also used to post negative information about Farhad Azima on the social blogging platform Reddit (https://www.reddit.com/user/Aabid236) (**JR1/31-32**). The first Reddit post was created on the 11th of August 2016, shortly after the publication of the torrent.

34. Based on bookmarking of all the pages by the same users and the use of the same username on Reddit, this leads me to believe that the dissemination of the hacked data would appear to have been done by one party only. Vikash confirmed to me that all the webpages and the subsequent bookmarks were created by Cyber Root.

35. Vikash explained that Mr. Sharma used the email "an_james@protonmail.ch" to upload the data through WeTransfer links.

36. I also note (from my own research) that Cyber Root has been engaged in a Search Engine Optimization (SEO) campaign to promote its own activities (**JR1/33-34**). In this regard, Cyber Root has used the same dissemination techniques used against Mr. Azima in order to promote its own activities. It has created a large amount of bookmarks on the website www.bookmark4you.com using the account 2287548-crriskadvisory, which it then links to various blogs and obscure pages in order to promote its activities. Cyber Root had also used Reddit via the username crriskadvisory, although its account is now suspended (**JR1/35-36**). It has also used wordpress and blogspot to push promotional materials on multiple occasions[13] (**JR1/37-50**), which is the same methodology deployed to push the hacked emails of Mr. Azima (**JR1/51-54**).

Vikash's cooperation and subsequent events

37. Vikash was initially quite forthcoming with information in my communications with him. He was almost boasting to me about his involvement in the project. However, as our relationship developed, he became increasingly concerned about where my questions were going. He also

[13] https://cyberrootcrgroup.wordpress.com/ / https://cyberroot-cr-group.blogspot.com/

told me that he was facing other legal troubles, having recently been accused of manslaughter. He became quite uncooperative and refused to engage much further with me.

38. Matters came to a head in the middle of September 2020 when I was told by Source 1 that Vikash had disclosed his conversations with me to the management of Cyber Root. I have had no direct communication with him since.

39. On 15 October 2020, Mr. Azima filed a Complaint in the US District Court (in North Carolina) against Nicholas Del Rosso and Vital Management Services Inc.

40. In late October 2020, I discovered that from Source 1 that Vikash had approached Cyber Root and had asked whether they would support him in case he got into legal trouble following the work he did for Cyber Root.

41. Cyber Root not only offered to support him for his legal expenses, but I understand from Source 1 that they have reportedly offered him a substantial sum and a percentage in the equity of Cyber Root, should Vikash decide to side with them.

42. Following Vikash's contact with Cyber Root, I understand from Source 1 that Cyber Root's directors reached out to all current and former employees of the company telling them that they are not to speak with anyone about the previous work they have done for the company and that they will be in great trouble should they decide to speak about the illegal methodology used by Cyber Root. I should say that I believe it was appropriate for me to seek information from Cyber Root employees about their work, given the unlawful acts that work entailed.

43. Furthermore, prior to Cyber Root's threat, Rajat (who I refer to above) had indicated that he was considering providing evidence for Mr. Azima. However, following Cyber Root's threat, he decided to revoke his offer to testify in these proceedings.

Cyber Root

44. From my own research into Cyber Root, I note the following:-

44.1 Cyber Root is a company registered in India on 13 August 2013. Its registered office address is: at 791 Sector-10A, Gurgaon, Haryana, India. The company is owned equally by Vijay Singh Bisht (the current managing director), Chiranshu Ahuja and Vibhor Sharma.

44.2 Cyber Root advertises itself as a cybersecurity actor and as an investigation firm. In multiple websites[14] (**JR1/55-67**), the company uses the same marketing material:

[14] https://www.crunchbase.com/organization/cr-risk-advisory / https://issuu.com/crriskadvisory/ / https://cyberrootcrgroup.wordpress.com/ / https://cyberroot-cr-group.blogspot.com/

"CR Risk Advisory is top notch Risk Management and Information Security provider." Other claims by the company are: "CR Group (CyberRoot Group) is holding company in the area of information security, cyber security solutions and Crisis Management Company. CR Group helps companies, government agencies and individuals reduce their exposure to risk and capitalize on business opportunities. CR Group (CyberRoot Group) offers expert support to Government, Legal, and Corporate institutions internationally. CyberRoot (CR) Group is there to protect client's business interests from all levels of risk, enabling corporates to perform at the top of their respective industries".

44.3 I note that in the initial version of the Memorandum of Association of the company dated 26th of July 2013, (**JR1/68-77**), the word "hacking" was mentioned in the object of the company:

"to carry on [...] hacking and risk averse software's [...]".

The wording was later removed on 02.08.2014 (**JR1/78-80**).

44.4 One employee of Cyber Root, Ms. Preeti Thapliyal (Information Security Analyst at Cyber Root) has worked/is working for the company BellTrox.

44.5 At **JR1/81** is a screenshot I took on 28 July 2020 of Ms. Thapliyal's LinkedIn page. I note that she states that she was engaged in phishing activities whilst working at BellTrox between August 2017 to the present day and that she joined Cyber Root in September 2018 to the present day.

"Worked on Custom Build Phishing Campaign Framework"; and

"created undetectable phishing Payloads."

It would therefore appear that Mr. Thapliyal splits her time between Cyber Root and BellTrox.

44.6 I have taken a further, more recent (on 8 February 2021) screenshot of the Ms. Thapliyal's Linked In page (**JR1/82**). This shows that the reference to Cyber Root has now been removed and replaced with the word 'confidential'. The text is otherwise the same.

44.7 At **JR1/83-84** is a 17 December 2018 copy of Ms. Thapliyal's Curriculum Vitae (redacted to remove personal data) which she provided to me as part of a job application process. I note that that she states in the section dealing with her work with BellTrox that she:

(a) "Worked on Custom Build Phishing Campaign Framework" and

(b) "Created undetectable phishing Payloads"

(c) It further confirms that she currently works for Cyber Root.

44.8 I am informed by Vikash that Cyber Root used to work closely with BellTrox. As I have explained above, BellTrox permitted Cyber Root to use BellTrox's phishing infrastructure (given that Cyber Root did not for some time have their own server to use for this purpose). In order to conduct a phishing attack, one needs to have a server available where a fake replicate of a webpage can be set-up. For example, if one wanted to fake the Facebook landing page, they would need to use a domain similar to the real facebook.com and would use, for example, loginfacebook.com. The landing page requires to be hosted on a server and the login data that is thus harvested needs to be stored somewhere. I understand from Vikash that Cyber Root used BellTrox's server for this purpose.

Statement of Truth

I believe that the facts stated in this witness statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed .....

JONAS REY

Date 11 February 2021

On behalf of: THE APPELLANT

Witness: Jonas Rey

1st witness statement

Date: 11 February 2021

Appeal No: A3/2020/1271

IN THE COURT OF APPEAL

(CIVIL DIVISION)

ON APPEAL FROM THE HIGH COURT OF JUSTICE, BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES, BUSINESS LIST [2020] EWHC 1327 (Ch) and [2020] EWHC 1686 (Ch) (Mr Andrew Lenon QC sitting as a Deputy Judge of the High Court)

BETWEEN:

FARHAD AZIMA

Appellant

- and -

RAS AL KHAIMAH INVESTMENT AUTHORITY

Respondent

FIRST WITNESS STATEMENT OF

JONAS REY

Burlingtons Legal LLP

5 Stratford Place

London

W1C 1AX

DX 82986 MAYFAIR

DH/AZI0003.2

Tel: 0207 529 5420

Solicitors for the Appellant

Exhibit F

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-CV-954

FARHAD AZIMA, Plaintiff, v. NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC., Defendants.	)	**DECLARATION OF VIKASH K. PANDEY**

I, **VIKASH K. PANDEY**, do hereby declare under penalty of perjury pursuant to 28 U.S.C § 1746 the following:

1. I am an information technology and cybersecurity professional and I reside in India.

2. I am also a former employee of CyberRoot Risk Advisory Private, Limited ("CyberRoot"). CyberRoot is an Indian company that provides risk mitigation, online reputation management, information security, and digital forensics services. I worked at CyberRoot from approximately July 2016 through May 2020.

3. In August 2020, I was contacted by Aditya Jain who falsely accused me of being involved in the alleged hacking Farhad Azima. Jain representated he was assisting Burlington Legal LLP and working on behalf of Farhad Azima.

4. Jain warned me that I was the primary suspect in an investigation into the hacking of Azima. He also told me that I was the primary suspect because Holden claimed

VKP.
Initials

that he identified an individual who worked at CyberRoot and BellTroX Info Tech Services ("BellTroX") and had used my name in the alleged hacking of Azima.

5. I denied the accusations and dismissed them as either a mistake or a fabrication.

6. I did not hack or assist in the hacking of Farhad Azima.

7. I did not work on any projects directed at or related to Azima.

8. I do not know who hacked Azima or if Azima was hacked.

9. While I worked at CyberRoot, CyberRoot did not engage in any illegal hacking activities.

10. I do not believe that CyberRoot would be involved in illegal hacking operations, including the alleged hacking of Azima.

Demand Letters and Threats of Legal Action

11. On August 28, 2020, I received a demand letter from Holden on behalf of Azima. A true and accurate copy of Holden's demand letter, which is dated August 20, 2020, is attached hereto as **Exhibit A**.

12. Holden claimed to be "in possession of information which confirms that [I was] involved and, indeed, [was] instrumental to" the alleged hacking of Azima. Holden also claimed to be "aware that [I am] not the sole player in the Hack and that [I was] performing [my] role on the instructions [I] had received from [my] client." These accusations are false and fabricated.

VPD.
Initials

13. While Holden did not disclose what information Azima possessed or identify my alleged client, he offered me a single opportunity to cooperate with his investigation and to provide a witness statement to avoid criminal and legal proceedings.

14. I immediately called a former colleague at CyberRoot – Chiranshu Ahuja – to determine whether he was aware of any security projects that related to Azima or work that could have been mistaken for the illegal acts of which Holden accused me.

15. I confirmed to Ahuja that I did not hack Azima and that I did not believe that CyberRoot engaged in any illegal activity. I also confirmed my recollection that CyberRoot did not work on matters related to Azima. Ahuja agreed with my recollection and believed that Holden was mistaken.

16. I also called Jain to notify him of Holden's demand letter. Jain, who I understood was acting for Holden, confirmed that he would coordinate with Holden regarding their demand that I provide testimony to avoid legal proceedings. Jain did, in fact, contact and assist Holden in Burlington's demands to me.

17. On or about August 31, 2020, Holden presented a Confidentiality Agreement to me by email and, separately, through Jain. A true and accurate copy of the Confidentiality Agreement is attached hereto as **Exhibit B**. At that time, my father was unwell and was receiving treatment.

18. Over the next week, Holden and Jain pressured me to sign the Confidentiality Agreement Holden refused to share any information supporting their accusations of me until I signed the Confidentiality Agreement. Apparently at Holden's instruction, Jain also

VKP.
Initials

urged me to sign the Confidentiality Agreement because Azima's representatives, including Holden, would immediately commence criminal and legal charges against me if I did not comply.

Repeated Demands for Testimony to Avoid Legal Proceedings

19. After several days of pressuring by Holden and Jain, I explained that I could not sign the Confidentiality Agreement because I was with my father who was sick and did not have acess to a printer. However, I understand that Jain signed the Confidentiality Agreement with my name on September 2, 2020.

20. I did not hack Azima and I do not believe that CyberRoot hacked Azima, but I feared that cooperating with Holden was the only way that I could confront the evidence that he claimed as support for his false accusations. Although I told Jain, as Holden's intermediary, that I would agree to the Confidentiality Agreement, I believe that my agreement was obtained under duress and false pretenses, as Azima's representatives refused to provide any evidence to support their accusations.

21. On September 2, 2020, Jain arranged a Zoom audio call between me, Jain, and a legal representative of Azima. I do not know Holden's voice, so I cannot confirm whether he was on this call; however, I understood and reasonably believe that I spoke to Holden or another member of Azima's legal team with Burlingtons during this call.

22. During this call, the Burlingtons representative told me that I needed to admit to being instrumental to the hack of Azima. He also claimed that he had evidence against

VRP.
Initials

me related to the hack of Azima and accused me of being associated with BellTroX, which he claimed was also responsible for the hack of Azima. These accusations were false.

23. I am not and have never been associated with BellTroX, and I denied any association with BellTroX.

24. I am not and have never been involved in the hacking of Azima, and I denied any involvement in the hacking of Azima.

25. Prior to these accusations, I did not know anything about the hacking of Azima, and I denied having any knowledge of the alleged hacking of Azima.

26. I demanded that I be provided with the evidence that was promised to me if I signed the Confidentiality Agreement. Jain and the Burlingtons representative refused to provide any evidence of my involvement, despite insisting that I sign the Confidentiality Agreement for that purpose.

27. I do not believe that Azima or his representatives had any evidence to support their accusations and demands to me. Rather, I believe that Holden and Jain insisted on the Confidentiality Agreement because they intended to pressure me to give false testimony during this call.

28. Despite the falsity of these accusations and my denial of the accusations, they continued to threaten criminal and other legal battles against me unless I agreed to provide testimony for Azima's benefit. They also told me that I would be compensated very well if I provided false testimony and implicated others.

Initials

Repeated Demands that I Sign a Consultancy Agreement and Implicate Others

29. On September 4, 2020, Dominic Holden provided a draft "Consultancy Agreement" to me and continued to pressure me to sign it to avoid legal proceedings. True and accurate copies of messages sent by Holden using his Burlingtons email address, dominic.holden@burlingtons.legal, are attached hereto as **Exhibit C**. Jain also provided a copy of the Consultancy Agreement to me on behalf of Holden, and I understood that Jain was acting as Holden's translator and authorized representative.

30. The first draft of the Consultancy Agreement included false representations that I was knowledgeable about the hacking of Azima. As I had previously denied having knowledge of or involvement in the hacking of Azima, I refused to sign the first draft of the Consultancy Agreement.

31. Later that day, Holden provided a revised version of the "Consultancy Agreement" to me. A true and accurate copy of the revised draft of the Consultancy Agreement signed by Holden is attached hereto as **Exhibit D**. Jain also provided a copy of the revised Consultancy Agreement to me on behalf of Holden, and I understood that Jain was acting as Holden's translator and authorized representative.

32. Under the revised Consultancy Agreement, Burlingtons offered to pay me to assist them in Azima's legal proceedings against the Ras Al Khaimah Investment Authority, including High Court Claim No. HC-2016-002798.

√ KP.
Initials

33. Burlingtons forecasted that I would be compensated for up to 30 hours of service per calendar month. The Consultancy Agreement provided that I would be paid $550 per hour and that agreement would continue for at least 18 months.

34. Holden delivered the Consultancy Agreement to me with his signature on behalf of Burlingtons.

35. All versions of the Consultancy Agreement indicated that I would be subject to reputational harm and that I would require protection.

36. Holden and Jain continued to pressure me to sign the Consultancy Agreement, even though the drafts included statements that I had previously denied and for which Holden did not provide supporting evidence.

37. Holden and Jain insisted that I falsely implicate others, including CyberRoot, in the hacking of Azima in exchange for payment under the Consultancy Agreement. Holden demanded that I agree to statements that I had previously denied and for which Holden did not provide supporting evidence.

38. When I refused to sign the revised Consultancy Agreement, Jain approached me at Holden's instruction and told me that I should focus on the money that I would be able to make if I signed the Consultancy Agreement. Jain estimated that I would be paid INR 3.3 crore (over $500,000) if I signed the revised Consultancy Agreement. Jain also assured me that he too would be paid if I signed the Consultancy Agreement.

39. When I refused to sign the revised Consultancy Agreement, Holden and Jain continued to threaten legal action against me if I did not sign the Consultancy Agreement.

VKP.
Initials

A true and accurate copy of a message that Holden sent to me threatening to bring legal proceedings against me if I did not sign the Consultancy Agreement is attached hereto as **Exhibit E**.

40. I refused to sign the Consultancy Agreement on the basis that the information and admissions that Holden sought from me was false, and I understood that the proposed payments to implicate CyberRoot were intended to frame CyberRoot in the hacking of Azima.

41. I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 22, 2020 in Dehli, India.

Vikash K. Pandey

Initials

Exhibit A

BURLINGTONS

MORE THAN LAW

Mr. Vikash Kumar Pandey
S/O Narmda Pasad Pandey, 272
N Pa Pasan, Pasan, Maharani
Laxmi Ward No 12, Kotma
Anuppur
Madhya Pradesh – 484336

Date: 20 August 2020
Our Ref: DH/AZI0003.2

Dear Sir,

RE: OUR CLIENT: MR. FARHAD AZIMA

We act for Mr. Farhad Azima.

Background

In August 2016, Mr. Azima's private and confidential data was published on the internet after it was illegally obtained by a cyber security hack (**"the Hack"**).

As a result of the dissemination of his data, he has suffered substantial damage to his reputation and earning potential. We estimate that his losses amount to in excess of $20,000,000.

Your role

We are in possession of information which confirms that you were involved and, indeed, were instrumental to the Hack. This is a very serious matter and you are liable to compensate Mr. Azima for the damage he has suffered as a result of the Hack.

We are however aware that you are not the sole player in the Hack and that you were performing your role on the instructions you had received from your client.

In the circumstances, we are offering you a single opportunity to co-operate with Mr. Azima's legal team to reveal the identity of the client who instructed you to hack Mr. Azima and to provide a Witness Statement sworn by a statement of truth explaining (1) your role in the Hack (2) the means by which the Hack occurred and (3) on whose instructions you were acting.

You have 3 days on receipt of this letter to respond to this request. If we have not received a satisfactory reply that you will co-operate willingly, our client will proceed with legal proceedings against you.

[redacted] 5 Stratford Place, London W1C 1AX

Representative offices:
Almaty, Geneva, Gibraltar, Malta, Moscow, St. Petersburg

Tel: +44 (0) 207 529 5420
Fax: +44 (0) 207 495 7450
DX: 82986 Mayfair
Web: www.burlingtons.legal

We urge you to take legal advice on the contents and effect of this letter.

All our client's rights and remedies are reserved.

Yours faithfully,

Dominic Holden

BURLINGTONS LEGAL LLP

Exhibit B

STRICTLY PRIVATE, CONFIDENTIAL AND PRIVILEGED

Confidentiality Agreement

BURLINGTONS

5 Stratford Place, London, W1C 1AX
Tel: 0207 529 5420 Fax: 0207 495 7450
www.burlingtonsllp.com

Ref: DH/AZI

CONTENTS

CLAUSE

This agreement is dated .....

Parties

(1) Burlingtons Legal LLP incorporated and registered in England and Wales with company number OC360876 whose registered office is at 5 Stratford Place, London, W1C 1AX (**Party 1**).

(2) Vikash Kumar Pandey of S/O Narmda Prasad Pandey, 272 N Pa Pasan, Pasan, Maharani Laxmi Ward No 12, Kotma, Anuppur, Madhya Pradesh – 484336 (**Party 2**).

BACKGROUND

(A) The parties intend to enter into discussions relating to the Purpose which will involve the exchange of Confidential Information between them.

(B) The parties have agreed to comply with this agreement in connection with the disclosure and use of Confidential Information.

Agreed terms

1. Interpretation

1.1 Definitions:

Business Day: a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

Confidential Information: has the meaning given in clause 2.

Discloser: a party to this agreement when it discloses its Confidential Information, directly or indirectly, to the other party.

Group: in relation to a company, that company, any subsidiary or any holding company from time to time of that company, and any subsidiary from time to time of a holding company of that company. Each company in a Group is a member of the Group.

Group Company: in relation to a company, any member of its Group.

Holding company: has the meaning give in clause 1.2(e).

Purpose: to assist in relation to ongoing litigation (including arbitration and other forms of dispute resolution fora) concerning Party 1 and / or Party 1's clients.

Recipient: a party to this agreement when it receives Confidential Information, directly or indirectly, from the other party.

Representative(s): in relation to each party and any member of its Group:

a) its officers and employees that need to know the Confidential Information for the Purpose;

b) its professional advisers or consultants who are engaged to advise that party and/or any member of its Group in connection with the Purpose;

c) its contractors and sub-contractors engaged by that party and/or any member of its Group in connection with the Purpose; and

d) any other person to whom the other party agrees in writing that Confidential Information may be disclosed in connection with the Purpose.

Subsidiary: has the meaning given in clause 1.2(e).

1.2 Interpretation.

(a) A reference to a statute or statutory provision is a reference to it as amended or re-enacted. A reference to a statute or statutory provision includes any subordinate legislation made under that statute or statutory provision, as amended or re-enacted.

(b) Any words following the terms **including**, **include**, **in particular**, **for example** or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

(c) A reference to **writing** or **written** includes fax and email.

(d) A reference to a **company** shall include any company, corporation or other body corporate, wherever and however incorporated or established.

(e) A reference to a **holding company** or a **subsidiary** means a holding company or a subsidiary (as the case may be) as defined in section 1159 of the Companies Act 2006 and a company shall be treated, for the purposes only of the membership requirement contained in section 1159(1)(b) and (c), as a member of another company even if its shares in that other company are registered in the name of:

(i) another person (or its nominee) by way of security or in connection with the taking of security; or

(ii) its nominee.

(f) Any obligation on a party not to do something includes an obligation not to allow that thing to be done.

2. Confidential Information

2.1 Confidential Information means all confidential information relating to the Purpose which the Discloser or its Representatives or any of its Group Companies, or their

Representatives directly or indirectly discloses, or makes available, to the Recipient or its Representatives or any of its Group Companies, or their Representatives, before, on or after the date of this agreement. This includes:

(a) the fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations;

(b) the existence and terms of this agreement;

(c) all confidential or proprietary information relating to:

(i) the business, affairs, customers, clients, suppliers, plans, intentions, or market opportunities of the Discloser or of any of the Discloser's Group Companies; and

(ii) the operations, processes, product information, know-how, technical information, designs, trade secrets or software of the Discloser, or of any of the Discloser's Group Companies;

(d) any information, findings, data or analysis derived from Confidential Information; and

(e) any other information that is identified as being of a confidential or proprietary nature;

but excludes any information referred to in clause 2.2.

2.2 Information is not Confidential Information if:

(a) it is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by the Recipient or its Representatives or by any of the Recipient's Group Companies or their Representatives in breach of this agreement (except that any compilation of otherwise public information in a form not publicly known shall still be treated as Confidential Information);

(b) it was available to the Recipient on a non-confidential basis prior to disclosure by the Discloser;

(c) it was, is, or becomes available to the Recipient on a non-confidential basis from a person who, to the Recipient's actual knowledge, is not under any confidentiality obligation in respect of that information;

(d) it was lawfully in the possession of the Recipient before the information was disclosed by the Discloser; and

(e) the parties agree in writing that the information is not confidential.

3. Confidentiality obligations

3.1 In return for the Discloser making Confidential Information available to the Recipient, the Recipient undertakes to the Discloser that it shall:

(a) keep the Confidential Information secret and confidential;

(b) not use or exploit the Confidential Information in any way except for the Purpose;

(c) not disclose or make available any Confidential Information in whole or in part to any person, except as expressly permitted by, and in accordance with this agreement.

3.2 The Recipient shall establish and maintain adequate security measures (including any reasonable security measures proposed by the Discloser from time to time) to safeguard the Confidential Information from unauthorised access or use.

4. Permitted disclosure

4.1 Disclosure to Representatives.

(a) The Recipient may disclose the Confidential Information to its Representatives, any of its Group Companies, or their Representatives on the basis that it:

(i) informs those Representatives, Group Companies or their Representatives of the confidential nature of the Confidential Information before it is disclosed; and

(ii) takes reasonable steps to procure that those Representatives, Group Companies or their Representatives comply with the confidentiality obligations in clause 3.1 as if they were the Recipient.

(b) The Recipient shall be liable for the actions or omissions of the Representatives, any of its Group Companies or their Representatives in relation to the Confidential Information as if they were the actions or omissions of the Recipient.

5. Mandatory disclosure

5.1 Subject to the provisions of this clause 5, a party may disclose Confidential Information to the minimum extent required by:

(a) an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction;

(b) the rules of any listing authority or stock exchange on which its shares or those of any of its Group Companies are listed or traded; or

(c) the laws or regulations of any country to which its affairs or those of any of its Group Companies are subject.

6. Return or destruction of Confidential Information

6.1 At the reasonable written request of the Discloser, the Recipient shall:

(a) destroy all documents and materials containing, reflecting, incorporating or based on the Confidential Information; and

(b) to the extent legally and technically practicable, erase all the Confidential Information from its computer and communications systems and devices used by it, or which is stored in electronic form.

6.2 Nothing in clause **Error! Reference source not found.** shall require the Recipient to return or destroy any documents and materials containing or based on the Discloser's Confidential Information that the Recipient is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or the rules of any listing authority or stock exchange, to which it is subject. The provisions of this agreement shall continue to apply to any documents and materials retained by the Recipient pursuant to this clause 6.2.

7. No obligation to continue discussions

Nothing in this agreement shall impose an obligation on either party to continue discussions or negotiations in connection with the Purpose, or an obligation on each party, or any of its Group Companies to disclose any information (whether Confidential Information or otherwise) to the other party.

8. Ending discussions and duration of confidentiality obligations

8.1 If either party decides not to continue to be involved in the Purpose with the other party, it shall notify that other party in writing immediately.

8.2 Notwithstanding the end of discussions between the parties in relation to the Purpose pursuant to clause 8.1, each party's obligations under this agreement shall continue in full force and effect.

8.3 The end of discussions relating to the Purpose shall not affect any accrued rights or remedies to which either party is entitled.

9. No partnership or agency

9.1 Nothing in this agreement is intended to, or shall be deemed to, establish any partnership or joint venture between the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

9.2 Each party confirms it is acting on its own behalf and not for the benefit of any other person.

10. General

10.1 Assignment and other dealings. Neither party shall assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any of its rights and obligations under this agreement.

10.2 Entire agreement

(a) This agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

(b) Each party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this agreement. Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this agreement.

10.3 Variation. No variation of this agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

10.4 Waiver. No failure or delay by a party to exercise any right or remedy provided under this agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

10.5 Severance

(a) If any provision or part-provision of this agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this agreement.

10.6 Notices

(a) Any notice or other communication given to a party under or in connection with this agreement shall be in writing and shall be:

(i) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

(ii) sent by email to the following addresses:

(A) Party 1: *dominic.holden@burlingtons.legal*

(B) Party 2: *vikz.hax@gmail.com*

(b) Any notice or communication shall be deemed to have been received:

(i) if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address; and

(ii) if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting or at the time recorded by the delivery service; and

(iii) if sent by email, at the time of transmission, or, if this time falls outside business hours in the place of receipt, when business hours resume. In this Clause 10.6(b)(iii), business hours means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the place of receipt.

(c) This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

(d) A notice given under this agreement is not valid if sent by email.

10.7 **Third party rights**

(a) Unless it expressly states otherwise, this agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this agreement.

(b) The rights of the parties to rescind or vary this agreement are not subject to the consent of any other person.

10.8 Governing law. This agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

10.9 Jurisdiction. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

This agreement has been entered into on the date stated at the beginning of it.

Signed by Dominic Holden
and on behalf of **Burlingtons Legal LLP**

.....
Partner

Signed by
Vikash Kumar Pandey

.....

Exhibit C

Private, Confidential and Privileged - Subject to Contract

Inbox

Dominic Holden 4 Sep
to me

From Dominic Holden • dominic.holden@burlingtons.legal

To vikz.hax@gmail.com

Date 4 Sep 2020, 11:05 pm

Standard encryption (TLS).
See security details

Show pictures

Dear Vikash,

I attach our signed counterpart of the Consultancy Agreement.

Please could you sign and then return to me a copy of the complete signed version (scan and email is fine).

Please do not hesitate to telephone me to discuss – my contact details are below.

Kind regards,

Dominic Holden 4 Sep

to me

From Dominic Holden • dominic.holden@burlingtons.legal

To vikz.hax@gmail.com

Date 4 Sep 2020, 11:34 pm

Standard encryption (TLS).
See security details

Show pictures

Dear Vikash,

Further to my email below, I attach signed Confidentiality Agreement / NDA.

Please sign and return the complete, signed version to me (scan and email is fine).

Show quoted text

Exhibit D

DATED 04 SEPTEMBER 2020

VIKASH KUMAR PANDEY

- and -

BURLINGTONS LEGAL LLP

CONSULTANCY AGREEMENT

AGREEMENT IS MADE ON 04 **..... SEPTEMBER 2020**

BETWEEN:

(1) **Vikash Kumar Pandey** of S/O Narmada Pasad Pandey, 272 N Pa Pasan, Pasan, Maharani Laxmi Ward No 12, Kotma Anuppur, Madhya Pradesh - 484336 (**"the Consultant"**); (**"the Consultant"**); and

(2) **Burlingtons Legal LLP** incorporated and registered in England & Wales with company number OC360876 whose registered office is at 5 Stratford Place, London W1C 1AX ("**Burlingtons**").

WHEREAS:

(A) The Consultant is an IT expert and ex-employee of Cyber Root Risk Advisory Private Limited (**"CR"**).

(B) Burlingtons are the English solicitors acting for Mr. Azima who is the Defendant, Counterclaimant and Proposed Appellant in proceedings commenced by Ras Al Khaimah Investment Authority ("**RAKIA**") in the High Court in London under Claim No. HC-2016-002798 (the "**RAKIA Proceedings**"). The RAKIA Proceedings concern, amongst other matters, the hacking of Mr. Azima's emails in around 2015 / 2016 (**"the Hack"**).

(C) The Consultant has agreed to provide assistance to Burlingtons in relation to their investigation into the Hack (**"the Hacking Investigation"**).

(D) It is understood that by assisting Burlingtons with the Hacking Investigation (**"the Purpose"**) the Consultant is risking his reputation within the IT industry and his personal security and that the Consultant may be required to incur substantial costs to ensure that his personal security is protected.

(E) The Consultant has dedicated time, and will need to dedicate further time, to providing information and assistance in connection with the Hacking Investigation. It is agreed that the Consultant will be engaged for the Purpose on the terms set out below.

IT IS AGREED:

1. **INTERPRETATION**

1.1 In this Agreement:

"**Commencement Date**" means 1 August 2020;

"**Confidential Information**" means confidential or secret information relating to Mr. Azima and / or the Hacking Investigation, including, without limitation, the existence and terms of this Agreement and any communications between Burlingtons (and / or its agents and / or advisers) and the Consultant;

"**Services**" means the services described in clause 3.

1.2 In this Agreement, any reference to a statutory provision is a reference to the provision from time to time renumbered, amended, re-enacted or consolidated.

1.3 In this Agreement, unless the context otherwise requires:

(a) references to clauses are to clauses of this Agreement; and

(b) the headings to the clauses are for convenience only and do not affect the Agreement's construction or interpretation.

2. **APPOINTMENT**

2.1 With effect from the Commencement Date, Burlingtons has engaged the Consultant to perform the Services.

3. **SERVICES**

3.1 During his engagement under this Agreement, the Consultant will give information and assistance to Burlingtons and / or its agents in connection with the Hacking Investigation.

3.2 The Consultant acknowledges that this could involve, but is not limited to, assisting in relation to any regulatory or legal process, preparing witness statements and giving evidence in person.

3.3 Without prejudice to the generality of clause 3.1, the Consultant shall make himself available for meetings for up to 30 hours per calendar month (via Zoom or other form of agreed upon video conferring platform), such meetings to take place at Burlington's request upon giving the Consultant at least 3 business days' notice; and

3.4 The Consultant represents, warrants and agrees that:

(a) any information or assistance provided to Burlingtons pursuant to this Agreement will be complete and accurate, and will be given truthfully to the best of the Consultant's knowledge and belief.

(b) he is a former employee of CR and has knowledge of the practices of the company.

(c) The execution, delivery and performance of this agreement will not conflict with:-

(i) Any law or regulation applicable to him; and / or

(ii) Any agreement or instrument binding upon him.

3.5 The Consultant shall indemnify Burlingtons against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred arising out of or in connection with:-

(a) Any breach of the warranties contained in clause 3.4.

(b) Any breach of this agreement.

(c) The enforcement of this agreement.

(d) Any claim made against Burlingtons by a third party arising out of or in connection with the provision of the Services.

3.6 It is agreed that no information or documentation (except as required by an order of a court of competent jurisdiction, or pursuant to any proper order or demand made by any competent authority or body where Burlingtons is under a legal or regulatory obligation to disclose the information and / or documentation) provided by the Consultant pursuant to this Agreement will be used by Burlingtons (on behalf of Mr. Azima) in support of any, action, claim, or prosecution against the Consultant in relation to his liability for the Hack.

4. **REMUNERATION**

4.1 Subject to the terms of this Agreement, Burlingtons shall pay the Consultant the sum of $550 per hour (exclusive of any applicable VAT) in consideration for the provision of the Services for a period of at least 18 months.

4.2 Subject to Burlingtons' prior written approval, Burlingtons shall reimburse all reasonable expenses properly and necessarily incurred by the Consultant in the course of this Agreement, subject to production of receipts or other appropriate evidence of payment.

4.3 The payment referred to at paragraph 4.1 shall include all work undertaken and assistance provided to Burlingtons by the Consultant to the date of this Agreement.

4.4 The period of service referred to at paragraph 4.1 may be extended by written agreement between the parties.

5. **CONFIDENTIAL INFORMATION**

5.1 The Consultant will not, except with the prior written consent of Burlingtons or pursuant to an order of a court of competent jurisdiction, or pursuant to any proper order or demand made by any competent authority or body where the Consultant is under a legal or regulatory obligation to make such disclosure, or to the Consultant's lawyers, auditors or insurers on terms which preserve confidentiality:

(a) disclose or communicate to any person, firm or company;

(b) cause unauthorised disclosure of; or

(c) otherwise make use of,

any Confidential Information that he has or may have acquired in the course of his engagement (whether before, on or after the date of this Agreement) and will use his best endeavours to prevent the unauthorised disclosure or publication of such information. This obligation survives the termination of this Agreement.

5.2 The obligations in clause 5.1 will cease if the relevant Confidential Information comes into the public domain other than through the Consultant's default or negligence.

6. **TERMINATION**

6.1 Upon the termination of this Agreement for whatever reason, the Consultant will deliver up all property and any documents or other information belonging to Burlingtons (and / or to Mr. Azima), including any Confidential Information, whether held electronically or in hard copy, which is in the Consultant's possession or under his control. The Consultant will not retain any copies of any such property, documents or information without written permission from Burlingtons.

6.2 The termination of this Agreement will not affect any of the provisions of this Agreement that are expressed to operate or have effect after its termination (including without limitation clause 5.1) and will not prejudice the exercise of any right or remedy of either party that has accrued prior to termination.

7. **STATUS**

7.1 The relationship of the Consultant to Burlingtons will be that of independent contractor and nothing in this Agreement shall render him an employee, worker, agent or partner of Burlingtons and the Consultant shall not hold himself out as such.

7.2 This Agreement constitutes a contract for the provision of services and not a contract of employment and accordingly the Consultant shall be fully responsible for and shall indemnify Burlingtons for and in respect of:

(a) any income tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the performance of the Services, where the recovery is not prohibited by law. The Consultant shall further indemnify Burlingtons against all reasonable costs, expenses and any penalty, fine or interest incurred or payable by Burlingtons in connection with or in consequence of any such liability, deduction, contribution, assessment or claim; and

(b) any liability arising from any employment-related claim or any claim based on worker status (including reasonable costs and expenses) brought by the Consultant against Burlingtons arising out of or in connection with the provision of the Services.

8. **MISCELLANEOUS**

8.1 This Agreement contains the entire agreement and understanding of the parties and supersedes all prior agreements, understandings or arrangements (both oral and written) relating to the subject matter of the same.

8.2 If a provision of this Agreement is found to be illegal, invalid or unenforceable, then to the extent it is illegal, invalid or unenforceable, that provision will be given no effect and will be treated as though it were not included in this Agreement, but the validity or enforceability of the remaining provisions of this Agreement will not be affected.

8.3 This Agreement may be entered into in any number of counterparts and any party may enter into this Agreement by executing any counterpart. A counterpart constitutes an original of this Agreement and all executed counterparts together have the same effect as if each party had executed the same document.

8.4 The parties do not intend by virtue of this Agreement to confer any rights on any third party pursuant to the provisions of the Contracts (Rights of Third Parties) Act 1999, except that any Group Company shall be entitled to enforce this Agreement.

9. **APPLICABLE LAW AND JURISDICTION**

9.1 Any dispute arising out of or in connection with this contract, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause.

9.2 The number of arbitrators shall be one.

9.3 The seat, or legal place, of arbitration shall be London.

9.4 The language to be used in the arbitral proceedings shall be English.

9.5 The governing law of the contract shall be the substantive law of England & Wales.

Signed by **Burlingtons Legal LLP**)
)
)
)
)

Dominic Holden

Dominic Holden

Partner

04 September 2020

Signed by **Vikash Kumar Pandey**)
)
)
)
)

Exhibit E

Dear Vikash,

We note that we have not yet received from you a signed copy of the Consultancy Agreement (sent under cover of our email of 4 September 2020, timed at 19:04).

We are further concerned by reports that in recent days you have spoken to current employees of Cyber Root about this matter in clear breach of the Confidentiality Agreement you signed on 2 September 2020.

We reiterate the points made in our letter of 20 August 2020. Our client has suffered an egregious breach of his rights as a result of the hacking and he intends to bring proceedings against the individuals and entities responsible with the full force of the law.

Our client had understood that you wished to avoid legal proceedings being pursued against you and so had agreed to compromise and to co-operate on the basis discussed, as reflected in the Consultancy Agreement (by which our client will agree not to use the information you have provided against *you*).

Our client sincerely hopes that this remains the case and that you will agree to work with him in relation to this matter and litigation against you can be avoided. We therefore invite you to: (1) immediately confirm that you will henceforth comply fully with the Confidentiality Agreement; and (2) sign and return the Consultancy Agreement by 4pm tomorrow (Tuesday, 8 September 2020).

All of our and our client's rights are otherwise reserved, including to issue proceedings without further notice.